Universidade Federal de Sergipe
Departamento de Matemática
Programa de Mestrado Profissional em Matemática
em Rede Nacional - PROFMAT

Uma abordagem do ensino de congruência na educação básica

por

Ataniel Rogério Gonçalves Gomes
Mestrado Profissional em Matemática - Itabaiana - SE

Orientador: **Prof. Dr. Mateus Alegri**

Maio de 2015

Universidade Federal de Sergipe
Departamento de Matemática
Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Ataniel Rogério Gonçalves Gomes

Uma abordagem do ensino de congruência na educação básica

Dissertação submetida ao Corpo Docente do Programa de Mestrado Profissional em Matemática da Universidade Federal de Sergipe como requisito para a obtenção do título de Mestre em Matemática.

Orientador: **Prof. Dr. Mateus Alegri**

Maio de 2015

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Gomes, Ataniel Rogério Gonçalves
G633a Uma abordagem do ensino de congruência na educação básica / Ataniel Rogério Gonçalves Gomes ; orientador Mateus Alegri. – São Cristóvão, 2015.
76 f. : il.

Dissertação (Mestrado profissional em Matemática) - Universidade Federal de Sergipe, 2015.

1. Matemática - Estudo e ensino. 2. Matemática (Ensino fundamental). 3. Educação básica. 4. Congruências e restos. 5. Teoria dos números. 6. Teoria dos conjuntos. I. Alegri, Mateus, orient. II. Título.

CDU 51:373.3

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Uma abordagem do ensino de congruência na educação básica.

por

Ataniel Rogério Gonçalves Gomes

Aprovada pela Banca Examinadora:

Mateus Alegri
Prof. Dr. Mateus Alegri- UFS
Orientador

Alejandro Caicedo Roque.
Prof. Dr. Alejandro Caicedo Roque- UFS
Primeiro Examinador

Dayenne Halley Gomes Bezerra
Prof. Dr. Dayenne Halley Gomes Bezerra - UFS
Segundo Examinador

Itabaiana, 15 de Maio de 2015.

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Cristóvão. Tel. (00 55 79) 2105-6887
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat.ufs@gmail.com

Agradecimentos

À Deus, por tudo que sou, bem como pela força e proteção nas inúmeras viagens ao longo do curso.

À minha família, em especial os meus pais, Antônio e Risalva, pelo carinho e atenção dispensados a mim.

Ao Prof. Geraldo Luiz Lima, pelo estímulo e acompanhamento ao estudo da matemática desde a minha formação básica.

Aos professores do PROFMAT em Itabaiana-SE, em particular meu orientador Prof. Dr. Mateus Alegri, pela partilha do conhecimento e dedicação ao seu trabalho.

Aos meus amigos, em especial aos de caminhada, pelo convívio, paciência, integração e ajuda em inúmeros momentos.

Resumo

O advento, em 1801, da brilhante obra *Disquisitiones Arithmeticae* de *Carl Friedrich Gauss* (1777-1885) proporcionou elementos de extraordinária importância para a Teoria dos Números, entre eles o estudo de congruência, o qual atrai os olhares de diversos matemáticos até os dias atuais pela sua aplicação em diversas áreas, inclusive em temas do ensino básico, evidenciando a necessidade do seu estudo como ferramenta de aprendizagem algébrica. Sendo assim, o presente trabalho propõe abordar o estudo de congruência de forma sistemática, visando a sua contextualização na educação básica, através de uma proposta de sequência didática, e sua aplicação em problemas do cotidiano.

Palavras-chaves: estudo de congruência; contextualização na educação básica; sequência didática; aplicação em problemas do cotidiano.

Abstract

The advent in 1801 of the brilliant work *Disquisitiones Arithmeticae* of *Carl Gauss Friedrich* (1777-1885) provided extremely important elements to Number Theory, including the study of congruences, which attracts the eyes of many mathematicians to this day for its application in various areas, including basic education issues, highlighting the need of their study as algebraic learning tool. Therefore, this paper proposes to approach the study of congruence in a systematic way, in order to the context of basic education, by proposing didactic sequence, and their application to everyday problems.

Keywords: study of congruences; context of basic education; didactic sequence; application to everyday problems.

Sumário

Introdução

Este trabalho propõe o estudo de Congruências na Educação Básica, mais precisamente no Ensino Médio, visando possibilitar ao educando a contextualização de problemas do cotidiano envolvendo o assunto e facilitar a resolução de problemas algébricos aparentemente complexos, propiciando ao mesmo ferramentas matemáticas poderosas não previstas no currículo atual e que somente teriam acesso em alguns cursos do ensino superior.

A fim de evitar remeter o leitor em todo momento a outras obras, principalmente no que diz respeito à teoria matemática utilizada nesta obra, disponho de forma breve, numa sequência lógica, alguns conceitos fundamentais que alicerçam as disposições contidas no objeto principal deste trabalho. Nesta perspectiva, temos os dois primeiros capítulos, sendo o capítulo inicial, denominado Introdução à teoria dos conjuntos e o segundo capítulo, chamado de Aritmética dos Inteiros, preparando o leitor para os capítulos seguintes.

No capítulo 3, chamado Congruência e Aritmética Modular se expõe de forma minuciosa os conceitos, proposições e teoremas sobre a teoria de congruência, permitindo a descoberta de um instrumento matemático para a resolução de problemas do cotidiano, através da percepção de sua ligação íntima com a divisibilidade de números inteiros.

No quarto capítulo, com base nas teorias da Didática da Matemática, é construída uma Proposta de Sequência Didática sobre congruência na Educação Básica na tentativa de tornar o conhecimento acessível aos estudantes, servindo de elemento norteador para professores que desejem expor tal conhecimento aos seus alunos.

Por fim, no quinto e último capítulo, exponho minhas considerações finais sobre o processo de construção deste trabalho.

CAPÍTULO 1

Introdução à Teoria dos Conjuntos

Tendo em vista o estudo de Congruência estar intimamente relacionado ao de conjuntos, principalmente no que diz respeito aos conjuntos numéricos, faz-se necessário uma sistematização lógica e progressiva dos conceitos que sustentam esta teoria, sendo que a abordagem desta obra se limitará a dispor de apenas uma introdução à teoria dos conjuntos, no entanto, sem perder de vista o rigor matemático que permeia esta área da matemática.

1.1 Noções Iniciais

1.1.1 Conjuntos

Definição 1.1.1 *Um conjunto é qualquer coleção de objetos. Os objetos deste conjunto são chamados de elementos ou membros.*

Exemplo 1.1.1 *Seja X o conjunto em que seus elementos são as letras do alfabeto grego. O conjunto X pode ser descrito na linguagem matemática por $X = \{\alpha, \beta, \gamma, \ldots, \psi, \omega\}$.*

Como exemplos de conjuntos numéricos amplamente conhecidos, temos o conjunto dos números naturais, denotado por $\mathbb{N} = \{1, 2, 3, ...\}$, e o conjunto dos números inteiros, denotado por $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$.

Se A é um conjunto e a é um elemento de A, escrevemos $a \in A$ (a pertence a A), caso contrário, ou seja, a não seja um elemento de A, denotamos $a \notin A$ (a não pertence a A).

1.1.2 Subconjuntos

Definição 1.1.2 *Dado um conjunto A, B é dito ser um subconjunto de A se para todo $b \in B$, b é elemento de A. A notação que utilizamos é $B \subset A$ (B está contido em A). Quando B não é subconjunto de A, escrevemos $B \not\subset A$ (B não está contido em A).*

Exemplo 1.1.2 *Note que $\mathbb{N} \subset \mathbb{Z}$, no entanto, $\mathbb{Z} \not\subset \mathbb{N}$, pois no conjunto dos números naturais não se encontram números negativos.*

Se $A \subset B$ e $B \subset A$, todo elemento de A é elemento de B, e analogamente todo elemento de B é elemento de A, logicamente A = B. Este é o chamado Princípio da Extencionalidade.

Saliente-se que $\{a, b\} = \{b, a\}$, e que $A \not\subset \{\{A\}, B\}$, mesmo que $A \in \{A\}$ e $\{A\} \subset \{\{A\}, B\}$.

As vezes é muito mais simples descrever um conjunto através de uma (ou mais) propriedade(s) que o caracteriza do que listar um a um seus elementos. Assim, se $P(x)$ é uma propriedade que um certo elemento têm, denotamos o conjunto $\{x|P(x)\}$ (a barra | pode ser lida como "tal que") como o conjunto dos elementos x que possuem a propriedade P . Por exemplo, considere a reta do plano cartesiano que passa pela origem e tem inclinação de 45°. Podemos descrever este conjunto como $A = \{(x, y) \in \mathbb{R}^2 | y = x\}$.

Um conjunto não menos importante é o conjunto que não possui elementos, mais conhecido como o conjunto vazio, o qual é denotado por $\varnothing$. Note que dissemos que $\varnothing$ é o conjunto, ou seja, sugerimos que este conjunto seja único. Definindo $\varnothing = \{x \in A | x \notin A\}$ pode se provar a unicidade deste.

Seja A um conjunto não vazio, o próprio A e o $\varnothing$ são sempre subconjuntos de A. Chamaremos estes de subconjuntos triviais de A. A seguir trataremos de questões operacionais envolvendo conjuntos.

1.1.3 Operações com Conjuntos

Definição 1.1.3 *A união de dois conjuntos A e B denotada por $A \cup B$ é o conjunto dos elementos pertencentes a A ou B, em linguagem formal*

$$A \cup B = \{x | x \in A \text{ ou } x \in B\}.$$

Exemplo 1.1.3 *Se A é o conjunto dos números naturais pares, $A = 2\mathbb{N} = \{2n | n \in \mathbb{Z}\}$ e $B = \{2n+1 | n \in \mathbb{Z}\}$ é o conjunto dos números naturais ímpares, então $A \cup B = \mathbb{N}$.*

Definição 1.1.4 *Dados dois conjuntos A e B definimos o conjunto interseção de A com B como sendo o conjunto contendo todos os elementos que são comuns a A e B, e denotamos este por $A \cap B$. Em linguagem de conjuntos $A \cap B = \{x | x \in A, x \in B\}$.*

Exemplo 1.1.4 $\{0, 2, 6\} \cap \{3, 6, 8\} = \{6\}$

Definição 1.1.5 *Sejam A e B conjuntos, definimos a diferença $A - B$ como o conjunto de todos os elementos que pertencem à A mas não pertencem à B, ou seja,*
$A - B = \{x | x \in A; x \notin B\}$.

Exemplo 1.1.5 *Seja C um conjunto não vazio e $D = \varnothing$, $C - D = C - \varnothing = C$, pois todo elemento pertencente à C não pertence ao vazio.*

Saliente-se que, geralmente, $A - B \neq B - A$, um exemplo disso, $\mathbb{N} - \mathbb{Z} = \varnothing$, porém, $\mathbb{Z} - \mathbb{N} = \mathbb{Z}^- \cup \{0\}$, em que $\mathbb{Z}^-$ representa o conjunto dos inteiros negativos.

Definição 1.1.6 *Sejam A e B conjuntos, com $B \subset A$, o conjunto complementar de B em relação a A é denotado por $\complement_A^B$, em que $\complement_A^B = A - B$.*

Exemplo 1.1.6 *Dados $X = \{a, b, c, d, e\}$ e $Y = \{a, e\}$, em que $Y \subset X$, temos que $\complement_X^Y = \{b, c, d\}$.*

1.2 Produto Cartesiano

Tratemos inicialmente da definição de par ordenado. Notemos que, conforme explicitado anteriormente, $\{a, b\} = \{b, a\}$, isto é, $\{a, b\}$ não é um par ordenado. Passemos agora à definição de par ordenado. A definição abaixo é atribuída à Kuratowski[1].

Definição 1.2.1 *O par ordenado (a, b) é definido como sendo o conjunto $\{\{a\}, \{a, b\}\}$.*

O teorema a seguir, demonstra que, de fato, (a, b) é um par ordenado.

Teorema 1.2.1 *$(a, b) = (x, y)$ se, e somente se, $a = x$ e $b = y$.*

Demonstração.

($\Leftarrow$) Se $a = x$ e $b = y$, obviamente, $(a, b) = (x, y)$.

($\Rightarrow$) Assumindo $(a, b) = (x, y)$, temos $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$. Deste modo, temos que $\{a\} \in \{\{x\}, \{x, y\}\}$. Se $\{a\} = \{x\}$, obrigatoriamente b = y. Porém, se $\{a\} = \{x, y\}$, então, $a = x = y = b$, demonstrando assim o teorema. ❑

Desta forma, agora podemos definir o produto cartesiano de maneira formal, conforme enunciado abaixo.

Definição 1.2.2 *Dados os conjuntos A e B, o produto cartesiano denotado por $A \times B$, é definido por*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Exemplo 1.2.1 *O plano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$ é um exemplo de produto cartesiano.*

A seguir definiremos os subconjuntos do produto cartesiano, denominados de relações.

[1]Kazimierz Kuratowski (1896-1980) foi um matemático polonês, membro da Escola de Matemática de Varsóvia.

1.2.1 Relações

Definição 1.2.3 *Sejam A e B conjuntos, uma relação entre A e B é um subconjunto de $A \times B$.*

Exemplo 1.2.2 *Uma reta qualquer no plano é uma relação em $\mathbb{R}^2$.*

Estudaremos em seguida algumas propriedades das relações em A (neste caso subconjuntos do cartesiano $A \times B$).

Definição 1.2.4 *Seja A um conjunto não vazio, uma relação de equivalência em A é uma relação S de A em A ($S \subset A \times A$) que satisfaz as seguintes condições*

1) $(a, a) \in S$, para qualquer $a \in A$. (Reflexividade)

2) Se $(a, b) \in S$, então $(b, a) \in S$, para quaisquer $a, b \in A$. (Simetria)

3) Se $(a, b) \in S$ e $(b, c) \in S$, então $(a, c) \in S$, para quaisquer $a, b, c \in A$. (Transitividade)

Podemos afirmar que a relação de equivalência enunciada acima é uma relação binária em A, visto que associa dois elementos de A. Sendo assim, outra maneira de definir uma relação de equivalência é

Definição 1.2.5 *Uma relação binária S em A é uma relação de equivalência se*

1) aSa, para quaisquer $a \in A$. (Reflexividade)

2) Se aSb, então bSa, para quaisquer $a, b \in A$. (Simetria)

3) Se aSb e bSc, então aSc, para quaisquer $a, b, c \in A$. (Transitividade)

Exemplo 1.2.3 *A relação de semelhança de triângulos determina uma relação de equivalência no conjunto de triângulos no plano. De fato, seja S a relação de semelhança de triângulos no plano, sejam t_1, t_2 e t_3 triângulos quaisquer no plano,*

i) *t_1 é auto-semelhante, isto é, $t_1 S t_1$;*

ii) *Se $t_1 S t_2$, é obvio que $t_2 S t_1$;*

iii) *Se $t_1 S t_2$ e $t_2 S t_3$, então $t_1 S t_3$, garantindo a transitividade.*

Geralmente, utiliza-se a notação $\sim$ para representar uma relação de equivalência, assim, se a e b estão relacionados, escrevemos que $a \sim b$, caso contrário, escrevemos que $a \not\sim b$.

O conjunto de todos os elementos que estão relacionados com $a \in A$ via $\sim$ é chamado de classe de equivalência de a, mais precisamente:

Definição 1.2.6 *Dado A um conjunto e $\sim$ uma relação de equivalência em A, então definimos a classe de equivalência de $a \in A$ via $\sim$ por*

$$\bar{a} = \{b \in A : \ b \sim a\}$$

A proposição abaixo é de extrema importância, pois caracteriza completamente uma classe de equivalência.

Proposição 1.2.1 *Dado um conjunto A e $\sim$ uma relação de equivalência em A, temos que:*

a) $\bar{a} = \bar{b}$ *se e somente se,* $a \sim b$.

b) Se $\bar{a} \neq \bar{b}$, *então* $\bar{a} \cap \bar{b} = \varnothing$.

Demonstração.

a) De acordo com o enunciado, temos

($\Rightarrow$) *Se* $\bar{a} = \bar{b}$, $a \in \bar{b}$, *ou seja,* $a \sim b$.

($\Leftarrow$) *Se* $x \in \bar{a}$, *então* $x \sim a$ *e* $a \sim b$, *pela transitividade,* $x \sim b$, *logo* $x \in \bar{b}$, *e portanto* $\bar{a} \subset \bar{b}$. *Analogamente, provamos que* $\bar{b} \subset \bar{a}$. ❑

b) Se $\bar{a} \cap \bar{b} \neq \varnothing$, *ou seja, suponhamos algum elemento* $x \in \bar{a} \cap \bar{b}$, *então* $a \sim x$ *e* $x \sim b$, *pela transitividade, temos que* $a \sim b$, *e pelo item anterior,* $\bar{a} = \bar{b}$. *Assim, pela contrapositiva de* $\bar{a} \cap \bar{b} \neq \varnothing \Rightarrow \bar{a} = \bar{b}$, *temos que se* $\bar{a} \neq \bar{b}$, *então* $\bar{a} \cap \bar{b} = \varnothing$. ❑

Observação 1.2.1 *Outra forma de descrevermos o item a) desta proposição é que uma classe de equivalência independe do representante da classe.*

Um dos objetivos para estudarmos relações de equivalência em A é que esta faz uma partição em A. Rigorosamente uma partição P de A é um conjunto de subconjuntos não vazios e disjuntos de A, tais que $\bigcup_{B\in P} B = A$.

Definição 1.2.7 *Uma partição P de A é um conjunto tal que*

P_1) Dois conjuntos distintos em P não tem elementos em comum;

P_2) Cada elemento de A está em algum elemento de P.

Tendo em mente a proposição anterior podemos estabelecer que uma relação de equivalência $\sim$ dada em um conjunto A determina uma partição do conjunto A. Se defirmos o conjunto de todas as classes de equivalência como a seguir, teremos uma partição do conjunto A via a relação de equivalência $\sim$.

Definição 1.2.8 *Dado um conjunto A e uma relação de equivalência $\sim$, o conjunto de todas as classes de equivalência via $\sim$ sobre A, denotada por $\frac{A}{\sim}$ é o conjunto*

$$\frac{A}{\sim} = \{\bar{a} | a \in A\}.$$

Apoiados pela proposição 1.2.1, temos que $\frac{A}{\sim}$ é uma partição de A. De fato, se $c \in \bar{a} \cap \bar{b}$, utilizando a parte b) da proposição citada pode-se provar que $a \sim b$, e pela parte a), $\bar{a} = \bar{b}$. No caso, o conjunto $\frac{A}{\sim}$ é chamado de conjunto quociente de A pela relação de equivalência $\sim$.

Exemplo 1.2.4 *Considere a relação $\sim$ em $\mathbb{Z} \times \mathbb{Z}$, dada por $a \sim b$ se e somente se, a e b possuem o mesmo resto na divisão por 3. Observemos que $\bar{0} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}, \bar{1} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}, \bar{2} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$, assim, $\bar{0} \cap \bar{1} = \emptyset$, $\bar{0} \cap \bar{2} = \emptyset$ e $\bar{1} \cap \bar{2} = \emptyset$, como $0 \sim 3k, 1 \sim 3k+1, 2 \sim 3k+2$ para qualquer $k \in \mathbb{Z}$, assim $\bar{0} \cup \bar{1} \cup \bar{2} = \mathbb{Z}$.*

No exemplo anterior note que, se $a, b \in \bar{x}$, $x \in \{0, 1, 2\}$, então $3|a - b$. Trataremos esta relação de equivalência mais a fundo no Capítulo 3. A idéia de classe de equivalência tem o objetivo de particionar conjuntos, podemos utilizar inclusive conjuntos de cardinalidade infinita, como o apresentado acima.

1.2.2 Funções

Neste seção estudaremos uma relação específica em $A \times B$, onde A e B são conjuntos não-vazios.

Dados A e B conjuntos não-vazios, estudemos um subconjunto das relações em $A \times B$, denominado de funções.

Definição 1.2.9 *Dados conjuntos A e B não-vazios, uma função f é uma relação entre A e B tal que para todo $a \in A$, existe apenas um único $b \in B$ tal que o par $(x, y) \in f$.*

Geralmente, utiliza-se a notação $f : A \to B$ (lê-se: função f de A em B), em que o conjunto A é chamado de domínio (partida) e B de contradomínio (chegada) da função f. Além disso, denota-se $y = f(x)$, quando $y \in B$ e $(x, y) \in f$, sendo assim, o conjunto de todos os elementos $f(x)$, onde $x \in A$, representa o conjunto imagem de f, cuja notação é dada por $Im(f)$. Assim, $Im(f) = \{y | f(x) = y, x \in A\}$.

Observação 1.2.2 *Seja f uma relação, em que $f : A \to B$, para que f seja uma função, é suficiente mostrarmos que*

$$\forall a_1, a_2 \in A, a_1 = a_2 \Rightarrow f(a_1) = f(a_2).$$

Exemplo 1.2.5 *Seja $A = \{1, 2, 3\}$ e $B = \{3, 6, 9\}$, além disso, $f = \{(1, 3), (2, 6), (3, 9)\}$. Note que f é uma função que associa os elementos de A em B, sendo que neste caso $Im(f) = B$, ou seja, a imagem igual ao contradomínio.*

Uma função, geralmente, é definida através de uma regra algébrica, exemplificando temos: $f : \mathbb{Z} \to \mathbb{Z}$, em que $f(x) = 3x + 2$ é uma função de $\mathbb{Z}$ em $\mathbb{Z}$.

Definição 1.2.10 *Uma função $f : A \to B$ é dita ser injetora se para quaisquer dois elementos distintos de A, suas imagens são distintas. Sendo assim, a função f é injetora se $a_1 \neq a_2$, então $f(a_1) \neq f(a_2)$ para quaisquer a_1 e a_2 elementos de A.*

Observação 1.2.3 *Seja f uma função, $f : A \to B$. Para que a mesma seja injetora basta verificar a seguinte condição, que é a contrapositiva da implicação acima (Definição 1.2.10)*

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Exemplo 1.2.6 *Seja $f_1 : \mathbb{N} \to \mathbb{N}$ em que $f(x) = x^2$ é uma função injetora, pois a cada elemento do domínio está associado a um único elemento distinto de B. No entanto, $f_2 : \mathbb{Z} \to \mathbb{N}$ em que $f(x) = x^2$ não é uma função injetora, pois $-1, 1 \in \mathbb{Z}$ e $1 \in \mathbb{N}$, e $f(-1) = (-1)^2 = 1 = 1^2 = f(1)$, ou seja, dois elementos do domínio possuem a mesma imagem, em linguagem lógico-matemática $f(-1) = f(1) \Rightarrow$ -1 $\neq 1$, contrariando o disposto na observação 1.2.3.*

Notemos com o exemplo anterior a importância do domínio e contradomínio estarem bem definidos, já que modificando os mesmos podemos obter uma função diferente ou até mesmo apenas uma relação, por exemplo: $f_3 : \mathbb{N} \to 2\mathbb{N}$ em que $f(x) = x^2$ não é uma função, apenas uma relação, pois $3 \in \mathbb{N}$ e $f(3) = 3^2 = 9 \notin 2\mathbb{N}$, ou seja, existe um elemento do domínio que não está associado a nenhum elemento do contradomínio, o que contraria a definição de função (Definição 1.2.9).

Definição 1.2.11 *Uma função $f : A \to B$ tal que $B = Im(f)$ é dita ser uma função sobrejetora.*

Exemplo 1.2.7 *Seja a função $f : \mathbb{R} \to \mathbb{R}_+ \cup \{0\}$ tal que $f(x) = |x - 3|$, a mesma possui como imagem o conjunto dos números reais não negativos, sendo, portanto, sobrejetora.*

Observação 1.2.4 *Para que uma função $f : A \to B$ seja sobrejetora verifiquemos se para qualquer $b \in B$, existir um elemento $a \in A$ tal que $b = f(a)$, isto é, para cada $b \in B$, existe pelo menos um par $(a, b) \in$ f, geralmente utiliza-se o Princípio da Extencionalidade comentado anteriormente, mostrando que $B \subset Im(f)$ e $Im(f) \subset B$.*

Se f é uma função injetora e sobrejetora, dizemos que f é bijetora, exemplo disso, temos a função $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = x^3$.

Abordamos a seguir a definição de imagem inversa.

Definição 1.2.12 *Seja $f : A \to B$ uma função, se $b \in B$, a imagem inversa de via f é o conjunto $f^{-1}(\{b\}) = \{a \in A |\ f(a) = b\}$.*

Exemplo 1.2.8 *Seja $f : A \to B$ uma função tal que $f(x) = x^4 + 1$, sabendo que $A = \{2, 3, 4\}$ e $B = \{17, 82, 142, 257\}$, temos que $f^{-1}(\{82\}) = \{3\}$ e $f^{-1}(\{142\}) = \varnothing$.*

Proposição 1.2.2 *Se $f : A \to B$ e $g : Im(f) \to C$ são funções, então a composição de funções dada por $g(f(a))$ para cada $a \in A$ é também uma função em $A \times C$, denotada por $g \circ f : A \to C$.*

Demonstração. Notemos inicialmente que $g \circ f$ é uma relação em $A \times C$. Como f e g são funções, para todo $a \in A$ existe um único $b \in B$, tal que o par ordenado $(a, b) \in f$, assim como $g : Im(f) \to C$, em que $b = f(a)$, para todo $f(a) \in Im(f)$ existe um único $c \in C$ tal que $(f(a), c) \in g$. Portanto, $c = g \circ f(a)$ e a relação $g \circ f$ é uma função. ❑

Exemplo 1.2.9 *Dadas f e g funções, $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = x - 2$ e $g : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = 3x^2 - 4$, a função $g \circ f$ é dada por $g \circ f : \mathbb{R} \to \mathbb{R}$ tal que $g \circ f(x) = 3x^2 - 12x + 8$.*

A seguir, trataremos das operações binárias.

Definição 1.2.13 *Uma operação binária em um conjunto A é uma função de domínio e contradomínio A.*

Seja $\diamond$ uma operação em A, denotamos a imagem do par (a, b), em que $(a, b) \in A$, por

$$\begin{aligned} \diamond : A \times A &\to A \\ (a, b) &\longmapsto a \diamond b \end{aligned}$$

Como exemplos de operações binárias, muito bem conhecidas, temos a soma e produto de números inteiros, com efeito sejam tais operações dadas por:

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\longmapsto a + b \end{aligned}$$

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \longmapsto a \cdot b$$

Na sequência abordaremos outros exemplos que mostram a importância do estudo de operações binárias.

Exemplo 1.2.10 *Se M é o conjunto das matrizes de ordem 2×2, a soma de matrizes é um exemplo de operação binária. Seja a função $m : M \to M$, considere assim A e B matrizes de ordem 2×2 tal que $A = [a_{ij}]$ e $B = [b_{ij}]$, $1 \leq i, j \leq 2$, a soma das matrizes A e B definida como $A + B = [a_{ij} + b_{ij}]$ é uma operação binária em M.*

Exemplo 1.2.11 *A função $\otimes : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por*

$$\otimes (m, n) = m \otimes n = mn + m^5 \text{ é uma operação binária em } \mathbb{Z}.$$

No capítulo 3 utilizaremos operações binárias distintas das acima, e que dizem respeito sobre o estudo de congruência, foco deste trabalho.

CAPÍTULO 2

Aritmética dos Inteiros

Os conjuntos dos números naturais e inteiros, denotados por $\mathbb{N}$ e $\mathbb{Z}$, respectivamente, em que $\mathbb{N} = \{1, 2, 3, ...\}$ e $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$ servirão de base para nosso estudo a partir deste capítulo, enfatizando que não teceremos maiores considerações no que diz respeito a construção destes conjuntos, tendo em vista transcender aos objetivos deste trabalho.

Inicialmente, enunciaremos propriedades dos inteiros em suas operações básicas, e na sequência, trataremos de algumas técnicas fundamentais para demonstrações de proposições matemáticas, conhecidas como o princípio da indução finita, em suas duas versões.

Abordaremos a seguir propriedades aritméticas de $\mathbb{Z}$

Propriedades de $(\mathbb{Z}, +, .)$

Em $\mathbb{Z}$ *consideremos as duas operações binárias: a soma* $+$ *e o produto* $\cdot$*, assim, para todos os números inteiros a, b e c, valem*

1) $a + b = b + a$ (comutatividade da soma)

2) $(a+b)+c = a+(b+c)$ (associatividade da soma);

3) Dado $a \in \mathbb{Z}$, existe $0 \in \mathbb{Z}$ tal que $a+0 = a$. (existência do elemento neutro aditivo);

4) Dado $a \in \mathbb{Z}$, existe $-a \in \mathbb{Z}$ tal que $a+(-a) = 0$. (existência do elemento inverso aditivo);

5) $a \cdot (b+c) = a \cdot b + a \cdot c$ (distributividade);

6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto);

7) $a \cdot b = b \cdot a$ (comutatividade do produto);

8) Dado $a \in \mathbb{Z}$, existe $1 \in \mathbb{Z}$ tal que $a \cdot 1 = a$ (existência do elemento 1);

9) $a \cdot b = 0 \Leftrightarrow a = 0$ ou $b = 0$ (inexistência de divisores de zero em $\mathbb{Z}$).

Postulado 2.0.1 *O Princípio da Boa Ordem (P.B.O.). Um conjunto não vazio de números naturais (inteiros positivos) tem um menor elemento.*

O exemplo a seguir demonstra a importância do P.B.O. nos mais diversos problemas envolvendo inteiros positivos.

Exemplo 2.0.12 *Mostre que o conjunto A, em que* $A = \{n \in \mathbb{Z} |\ 0 < n < 1\}$ *é vazio.*

Demonstração. Suponha que A seja um conjunto não-vazio. Como $A \subset \mathbb{Z}_+$, pelo P.B.O. o conjunto A possui um menor elemento a, onde $0 < a < 1$. Multiplicando membro a membro da desigualdade por a temos que $0 < a^2 < a < 1$, assim, temos que $a^2 \in A$ e é menor que a, contradizendo a hipótese inicial. ❑

Assumindo o P.B.O. como postulado podemos demonstrar o Princípio de Indução Finita, em suas duas formas, como veremos na sequência.

Teorema 2.0.2 *O Princípio de Indução Finita em sua 1ª Forma (P.I.F.- 1ª Forma)*

Seja A um conjunto de números naturais, tal que

i) $1 \in A$;

ii) *Se $n \in A$, então $n+1 \in A$;*

Então $A = \mathbb{N}$.

Demonstração. Seja A um subconjunto de $\mathbb{N}$ em que valem *i)* e *ii)*. Suponhamos por contradição que A não contém todos os inteiros positivos. Seja $B \subset \mathbb{N}$ um conjunto não vazio em que todo elemento de B não é elemento de A. Pelo P.B.O existe $b \in B$, menor elemento de B. Como vale *i)*, $b > 1$, e assim $b-1 \in A$, e como vale *ii)* $b-1+1 = b \in A$, o que caracteriza a contradição. ❑

Teorema 2.0.3 *O Princípio de Indução Finita em sua 2ª Forma (P.I.F.- 2ª Forma)*

Seja A um conjunto de números naturais, tal que

i) $1 \in A$;

ii) *Se $2, 3, \ldots, n \in A$, então $n+1 \in A$;*

Então $A = \mathbb{N}$.

Demonstração. Seja A um conjunto em que valem as condições *i)* e *ii)* do P.I.F. - 2ª Forma. Suponhamos, por absurdo, que apesar de valer estas condições exista um conjunto B, $B \subset \mathbb{N}$, tal que $B - A$ é um conjunto não-vazio de números naturais. Assim, pelo P.B.O. B teria um menor elemento b, e de *i)*, sabemos que $1 \notin B$, segue que existe k natural, tal que $b = 1 + k > 1$. Logo, $1, 2, \ldots, b-1 \notin B$, ou seja, $1, 2, \ldots, b-1 \in A$. Mas, por *ii)*, temos que $b = (b-1) + 1 \in A$, um absurdo. ❑

2.1 Divisibilidade

Definição 2.1.1 *Se a e b são inteiros e $b \neq 0$, dizemos que a divide b se existir um inteiro c tal que $b = ac$, cuja notação é $a|b$.*

Observação 2.1.1 *Quando a não divide b, escrevemos que $a \nmid b$.*

Exemplo 2.1.1 $6|42$*, pois* $42 = 6 \cdot 7$*;* $11|165$*, pois* $165 = 11 \cdot 15$*; no entanto,* $7 \nmid 11$*, pois não existe* $x \in \mathbb{Z}$ *tal que* $11 = 7x$*.*

Observação 2.1.2 *Nesta obra não consideraremos a entidade* $0|0$.

Vamos citar algumas propriedades da divisibilidade em $\mathbb{Z}$.

Proposição 2.1.1 *Se o inteiro* a *divide todos os números inteiros pertencentes à lista* $c_1, c_2, \ldots, c_n$, *então* a *divide qualquer combinação do tipo* $\sum_{i=1}^{n} m_i c_i$, *onde* $m_i \in \mathbb{Z}$ *para todo* $1 \leq i \leq n$.

Demonstração. Utilizando o P.I.F - 1ª Forma, temos que se $a|c$, então $a|mc$ para todo $m \in \mathbb{Z}$, logo para o caso $n = 1$ a proposição é válida. Assumiremos a afirmação válida para n e provaremos a veracidade desta para $n + 1$.

Assim, se $a|c_1, c_2, \ldots, c_n, c_{n+1}$, por hipótese de indução $a|\sum_{i=1}^{n} m_i c_i$ para quaisquer $m_i \in \mathbb{Z}$, onde $1 \leq i \leq n$, então existe $l \in \mathbb{Z}$ tal que $\sum_{i=1}^{n} m_i c_i = la$. Como $a|c_{n+1}$, existe $b \in \mathbb{Z}$ satisfazendo $c_{n+1} = ab$.

Se $m_{n+1} \in \mathbb{Z}$, a soma $\sum_{i=1}^{n+1} m_i c_i = \sum_{i=1}^{n} m_i c_i + m_{n+1} \cdot c_{n+1} = la + m_{n+1} \cdot ab = a\,(l + m_{n+1} b)$ e por conseguinte $a|\sum_{i=1}^{n+1} m_i c_i$, como queríamos demonstrar. ❑

Proposição 2.1.2 *Se* $a, b, c \in \mathbb{Z}$, *então:*

1) $a|a$;

2) Se $a|b$ *então* $ac|bc$;

3) Se $ab|ac$ *então* $b|c$;

4) Se $a|b$ *e* $b \neq 0$, *então* $|a| \leq |b|$;

5) Se $a|b$ *e* $b|a$, *então* $|a| = |b|$;

6) Se $a|b$ *então* $\frac{b}{a}|b$;

7) Se $a|b$ *e* $b|c$, *então* $a|c$;

Tendo em vista as demonstrações serem triviais, omitimos as mesmas neste material, para consultá-las ver [5] e [9].

Proposição 2.1.3 *Se $a, b \in \mathbb{Z}, n \in \mathbb{N}$, e $b \neq a$, então $a - b | a^n - b^n$.*

Demonstração. Basta observar que $(a-b)\left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right) = a^n - b^n$. ❑

Proposição 2.1.4 *Se $a, b \in \mathbb{Z}, n \in \mathbb{N}$, e $b \neq -a$, então $a + b | a^{2n} - b^{2n}$.*

Demonstração. Observemos que $(a+b)\left(a^{2n-1} - a^{2n-2}b + \ldots + ab^{2n-2} - b^{2n-1}\right) = a^{2n} - b^{2n}$. ❑

Proposição 2.1.5 *Se $a, b \in \mathbb{Z}, n \in \mathbb{N}$, e $b \neq -a$, então $a + b | a^{2n+1} - b^{2n+1}$.*

Demonstração. Note que $(a+b)\left(a^{2n} - a^{2n-1}b + \ldots - ab^{2n-1} + b^{2n}\right) = a^{2n+1} - b^{2n+1}$. ❑

Teorema 2.1.1 (O algoritmo da divisão euclidiana em $\mathbb{Z}$). Sejam a e b inteiros, com $b \neq 0$, existem únicos inteiros q (quociente) e r (resto), onde

$$a = bq + r \text{ e } 0 \leq r < |b|.$$

Demonstração. Se $b|a$, tomemos $r = 0$, tornando válido o teorema. Suponhamos que $b \nmid a$ e $b < a$, e considere o conjunto $A = \{a - nb > 0 | n \in \mathbb{Z}\}$. Como A é não vazio (pelo menos $a - b \in A$), pelo P.B.O. o conjunto A tem um menor elemento $r = a - qb$. Provemos que $r < |b|$. Sendo assim, suponha que $r = a - qb > |b|$, assim, se $b > 0$, $a - (q+1)\, b > 0$, logo $a - (q+1)\, b \in A$, porém $a - (q+1)\, b < r$, absurdo. De maneira análoga, para $b < 0$, chegaremos em um absurdo.

Para o caso $b > a$, tome $q = 0$ e $r = a$, verificando a validade do enunciado acima.

Resta-nos provar a unicidade de q e r. Suponha que existam inteiros q_1, q_2, r_1, r_2 satisfazendo $a = bq_1 + r_1$ e $a = bq_2 + r_2$ com $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$. Igualando as equações, temos: $bq_1 + r_1 = bq_2 + r_2$, colocando b em evidencia têm-se $b\,(q_1 - q_2) = r_2 - r_1$. Sendo assim, $b | r_2 - r_1$, e pela proposição 2.1.2, item ④, $|b| \leq |r_2 - r_1|$, mas como $r_1 < r_2 < |b|$, temos que $|r_2 - r_1| < |b|$, e isto só é possível se $r_2 - r_1 = 0$, ou seja, $r_1 = r_2$. Substituindo o resto na equação $b\,(q_1 - q_2) = r_2 - r_1$, temos que $b\,(q_1 - q_2) = 0$, e como $\mathbb{Z}$ não possui divisores de zero (Propriedade 9), e por hipótese $b \neq 0$, temos que $q_2 - q_1 = 0$, o que implica $q_1 = q_2$. ❑

Exemplo 2.1.2 *Na divisão de* 732 *por* 35*, encontramos* $q = 20$ *e* $r = 32$*.*

Posteriormente, abordaremos o conceito de Máximo Divisor Comum de um conjunto de inteiros.

2.2 Máximo Divisor Comum

Definição 2.2.1 *Sejam* $a, b \in \mathbb{Z}$*, o máximo divisor comum de "a" e "b" é o maior inteiro positivo "d" que divide "a" e "b", cuja notação é* $d = m.d.c.\{a, b\}$*.*

Exemplo 2.2.1 $d_1 = m.d.c.\{4, 17\} = 1$*;* $d_2 = m.d.c.\{10, 25\} = 5$*.*

Mais adiante conheceremos uma ferramenta poderosa no cálculo de $m.d.c.'s$, capaz de facilitar o cálculo de m.d.c. de números de alta magnitude como

$$m.d.c\left\{\left(14^{38} + 14^{37} + \ldots + 14 + 1\right), 13\right\}, \text{ que é } 13.$$

Podemos definir de forma recursiva o $m.d.c.$ de uma lista de números inteiros.

Definição 2.2.2 *Se* $a_1, a_2, \ldots, a_n \in \mathbb{Z}$*, o* $m.d.c.\{a_1, a_2, \ldots, a_n\}$ *é o maior inteiro positivo* d *que divide todo* a_j *para* $1 \leq j \leq n$*.*

Teorema 2.2.1 *Se* $d = m.d.c.\{a, b\}$ *existem inteiros* m_0 *e* n_0 *tais que* $d = m_0 a + n_0 b$*, isto é,* d *pode ser escrito como uma combinação envolvendo* a *e* b*.*

Demonstração. Considere o conjunto de inteiros positivos $A = \{ma + nb |\ m, n \in \mathbb{Z}\}$. Observe que A possui infinitos elementos positivos, e por conseguinte pelo P.B.O. o conjunto A possui um menor elemento. Suponhamos $c = m_0 a + n_0 b$ o menor elemento. Provemos que c é um divisor comum de a e b e que de fato $c = d$, isto é, d é o menor inteiro positivo pertencente à A.

Se $c \nmid a$ pelo algoritmo da divisão existem inteiros q e r, onde $a = cq + r$ e $0 < r < c$. Assim, $r = a - cq = (1 - qm_0)\, a + (-qn_0)\, b \in A$, e $r < c$, contrariando a minimalidade de c, absurdo. De forma análoga pode-se provar que $c|b$.

Agora demonstremos que $d = c$. Como $d = m.d.c.\{a, b\}$, existem inteiros k e l

satisfazendo $a = dk$ e $b = dl$, e como $c = m_0a + n_0b$, temos $c = d\,(m_0k + n_0l)$, logo $d|c$, o que implica que $d \leq c$. Se $d = m.d.c.\{a, b\}$, não é verdade que $d < c$, restando apenas a possibilidade em que $d = c$. ❑

Observação 2.2.1 *Com efeito, se $d = m.d.c.\{a_1, a_2, \ldots, a_n\}$, por indução se demonstra que existem $k_1, k_2, \ldots, k_n \in \mathbb{Z}$ tais que $d = k_1a_1 + a_2k_2 + \ldots + k_na_n$. Adiante, quando exposto o conceito de ideais em $\mathbb{Z}$, veremos uma maneira mais simples e elegante de demonstrar tal fato.*

Observação 2.2.2 *Se $d = m.d.c.\{a, b\}$, então todo c que é divisor comum de a e b é divisor de d.*

Proposição 2.2.1 *Se $c \in \mathbb{N}$, então $m.d.c.\{ca, cb\} = c \cdot m.d.c.\{a, b\}$.*

Demonstração. Pelo teorema 2.2.1, temos que $d = m.d.c.\{a, b\}$ é o menor inteiro positivo em $A = \{ma + nb | m, n \in \mathbb{N}\}$. Desde que $c > 0$, dc é o menor inteiro positivo de $B = \{m\,(ca) + n\,(cb)\,| m, n \in \mathbb{N}\}$. Portanto, $cd = c \cdot m.d.c.\{a, b\} = m.d.c.\{ca, cb\}$. ❑

Corolário 2.2.1 *Se $c|a$ e $c|b$, então* $m.d.c.\left\{\frac{a}{c}, \frac{b}{c}\right\} = \frac{m.d.c.\{a, b\}}{c}$.

Demonstração. Tendo em vista a e b serem divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros, e pela proposição anterior temos que

$$m.d.c.\left\{\frac{a}{c}, \frac{b}{c}\right\} = \frac{1}{c} \cdot m.d.c.\{a, b\} = \frac{m.d.c.\{a, b\}}{c}.$$ ❑

Corolário 2.2.2 *Se $d = m.d.c.\{a, b\}$,* $m.d.c.\left\{\frac{a}{d}, \frac{b}{d}\right\} = 1$

Demonstração. Pelo corolário anterior e sabendo que $d = m.d.c.\{a, b\}$, temos que

$$m.d.c.\left\{\frac{a}{d}, \frac{b}{d}\right\} = \frac{m.d.c.\{a, b\}}{d} = \frac{d}{d} = 1.$$ ❑

Observação 2.2.3 *Quando $m.d.c.\{a, b\} = 1$ dizemos que a e b são primos entre si, ou ainda, coprimos.*

Proposição 2.2.2 *Se a e b são coprimos e $a|bc$ então $a|c$.*

Demonstração. Sendo a e b coprimos, temos que $m.d.c.\{a,b\} = 1$, ou seja, $a \nmid b$, e como $a|bc$, logo $a|c$. ❑

Exemplo 2.2.2 *Note que* $6|252 = 36 \cdot 7$*, mas* $6 \nmid 7$*, logo* $6|36$*.*

Demonstremos abaixo o lema de Euclides. Este lema faz-se interessante pelo uso técnico em se determinar m.d.c.'s de números muito grandes.

Lema 2.2.1 (O Lema de Euclides) Se $a, b, n \in \mathbb{Z}$, então

$$m.d.c.\{a,b\} = m.d.c.\{b, a-bn\}.$$

Demonstração. Seja A o conjunto dos divisores positivos de a e b, e B o conjunto dos divisores positivos de b e $a - bn$. Provemos que $A = B$.

Dado $c \in A$, $c|a, b$, logo c divide qualquer combinação envolvendo a e b, inclusive $a - bn$, logo $c \in B$. Reciprocamente, para todo $c \in B$, $c|b, a - bn$, logo $c|a - bn + bn = a$, assim, $c \in A$. Logo, $A = B$, o que implica que o $m.d.c.\{a,b\} = m.d.c.\{b, a-bn\}$. ❑

Exemplo 2.2.3 *Se* $a, n \in \mathbb{N}$*,* $a > 1$*, mostre que* $m.d.c.\left\{\frac{a^n-1}{a-1}, a-1\right\} = m.d.c.\{a-1, n\}$

Demonstração. Pela proposição 2.1.3, $a-1|a^n-1^n$, como $a^n - 1^n = a^n - 1$, temos que $a-1|a^n-1$, sabendo que $\frac{a^n-1}{a-1} = (a^{n-1} + a^{n-2} + \ldots + a + 1)$, observe que $a^{n-1} + a^{n-2} + \ldots + a + 1 = (a^{n-1} - 1) + (a^{n-2} - 1) + \ldots + (a-1) + n$, assim $a - 1$ divide todos as parcelas da última equação, exceto n.

Assim, se $c|a-1$, $c|\frac{a^n-1}{a-1}$ e $c|n$, pelo lema anterior temos que $m.d.c.\left\{\frac{a^n-1}{a-1}, a-1\right\} = m.d.c.\{a-1, n\}$. ❑

O exemplo a seguir é um exemplo numérico do resultado provado acima.

Exemplo 2.2.4 *Encontre o* $m.d.c\left\{\left(14^{38} + 14^{37} + \ldots + 14 + 1\right), 13\right\}$.

Solução. Como $(14^{38} + 14^{37} + \ldots + 14 + 1) = \frac{14^{39}-1}{14-1}$, conforme a demonstração acima, vale que:

$$m.d.c.\left\{\frac{14^{39}-1}{14-1}, 14-1\right\} = m.d.c.\{14-1, 39\} = m.d.c.\{13, 39\} = 13.$$

Teorema 2.2.2 (O algoritmo de Euclides) Se $r_0 = a$ e $r_1 = b$, onde $a \geq 0$ e $b > 0$, e se o algoritmo da divisão euclidiana for aplicado de forma sucessiva resultando em $r_j = q_{j+1}r_{j+1} + r_{j+2}$, onde $0 \leq r_{j+2} < r_{j+1}$, para $j = 0, 1, \ldots, n-1$ e r_n é o último resto não nulo. Então, $m.d.c.\{a, b\} = r_n$.

Demonstração. Dividindo $r_0 = a$ por $r_1 = b$, encontramos q_1 e r_1 inteiros onde $r_0 = q_1r_1 + r_2$, com $0 < r_2 < r_1$. Utilizando o algoritmo da divisão para dividir $b = r_1$ por r_2 têm-se que $r_1 = q_2r_2 + r_3$, onde $0 < r_3 < r_2$. Utilizando o Lema de Euclides, onde $r_2 = r_0 - q_1r_1$, temos que $m.d.c.\{a, b\} = m.d.c.\{r_1, r_2\}$, e pelo mesmo lema na segunda equação onde $r_3 = r_1 - q_2r_2$, temos que $m.d.c.\{r_2, r_3\} = m.d.c.\{r_1, r_2\}$. Aplicando o lema citado mais $n-2$ vezes, e notando que $r_n - 1 = q_nr_n + 0\,(r_{n+1} = 0)$,

$$m.d.c.\{a, b\} = m.d.c.\{r_1, r_2\} = m.d.c.\{r_2, r_3\} = \ldots = m.d.c.\{r_n - 1, r_n\} = r_n. \text{ ❑}$$

2.3 Números Primos

Definição 2.3.1 *Um número natural $p > 1$ é dito ser um número primo se $p|ab$ implicar $p|a$ ou $p|b$, isto é, toda vez que p divide um produto de números ab, p divide a ou b.*

A definição acima pode parecer diferente daquela que o seu professor do ensino fundamental lhe ensinou. Porém esta definição é análoga àquela de tempos atrás, como veremos abaixo. Utilizamos a dada definição para que trabalhando com estruturas mais abstratas possamos reconhecer certas propriedades equivalentes (ou quase) a números primos em $\mathbb{Z}$.

Proposição 2.3.1 *Um número inteiro $p > 1$ é primo se os únicos divisores de p é ± 1 e $\pm p$.*

Demonstração. Seja a um divisor de p (p primo), então existe $b \in \mathbb{Z}$ tal que $p = ab$, assim, $p|ab$, e pela definição 2.3.1 temos que $p|a$ ou $p|b$. Se $p|a$ então $a = pd$, o que implica que $p = ab = (pd)\,b$, assim $db = 1$, daí, $b = \pm 1$ e $d = \pm 1$ (nesse caso $a = \pm p$). Portanto, se p é primo então os únicos divisores de p são ± 1 e $\pm p$. ❑

Exemplo 2.3.1 *O número* 17 *é primo, pois os únicos divisores são* 1 *e* 17*, ao passo que* 4 *não é primo, pois os divisores dele são* $1, 2$ *e* 4*.*

Observação 2.3.1 *O número* 2 *é o único número primo par.*

Teorema 2.3.1 (Teorema Fundamental da Aritmética) *Todo inteiro maior do que* 1 *ou é primo ou pode ser representado como um produto de números primos e esta representação é única, a menos de ordenação.*

Demonstração. Inicialmente, se n é primo nada se tem a demonstrar. Suponha então n composto, e considere p_1 ($p_1 > 1$) o menor dos divisores positivos de n. De fato, p_1 é primo, pois se não o fosse existiria um certo p tal que $p_1 > p > 1$ com $p|n$, contradição. Portanto, $n = p_1 n_1$.

Novamente, se n_1 é primo nada se tem a demonstrar. Se n_1 for composto considere p_2 ($p_2 > 1$) como o menor divisor de n_1. Assim, analogamente a argumentação exposta, p_2 é primo e $n = p_1 p_2 n_2$.

Continuando o mesmo procedimento em finita vezes, obtemos uma sequência de inteiros positivos $n_1, n_2, \ldots, n_r$, assim, como a sequência de primos $p_1, p_2, \ldots, p_k$ pode não ser distinta, temos que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Provemos a unicidade da decomposição de n, a menos da ordem. Utilizando indução em n, temos que para $n = 2$ a proposição é válida. Admitamos válida para os inteiros maiores do que 1 e menores que n, então devemos provar a validade para n. Se n for primo a unicidade está provada. Supondo n composto, e que tenha duas fatorações, ou seja, $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$. Como p_1 divide o produto $q_1 q_2 \cdots q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade suponha que $p_1|q_1$, portanto, $\dfrac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_r$, como $1 < \dfrac{n}{p_1} < n$, assim, por hipótese as duas fatorações são idênticas, então $s = r$, logo as fatorações $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_r$ são iguais, a menos da ordenação. ❑

Observação 2.3.2 *Pelo teorema anterior, a fatoração pode ser representada por* $a \in \mathbb{N}$ *em que* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}$*, onde* p_i *é o i-ésimo número primo.*

Observação 2.3.3 *Se $a \in \mathbb{Z}$ com valor absoluto superior a 1, a é representado como $a = lp_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ onde $l \in \{-1, 1\}$ e $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ é a representação de $|a|$.*

Corolário 2.3.1 *Se $a = \prod_{i=1}^{n} p_i^{\alpha_i} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, o conjunto dos divisores positivos de A é o conjunto $A = \left\{ \prod_{i=1}^{n} p_i^{\beta_i} | 0 \leq \beta_i \leq \alpha_i, i = 1, 2, \ldots, n \right\}$*

Observação 2.3.4 *A partir do corolário acima fica fácil de calcular o número de divisores positivos $a > 1$. Seja d_n este número, se $a = \prod_{i=1}^{n} p_i^{\alpha_i}$, então*

$$d_n = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1).$$

A seguir mostraremos que a sequência de números primos é infinita.

Teorema 2.3.2 (Euclides) *Existem infinitos números primos.*

Demonstração. Suponhamos o contrário, ou seja, que os números primos sejam em quantidade finita. Consideremos $p_1, p_2, \ldots, p_k$ todos os primos. Seja $S = p_1 \cdot p_2 \cdots p_k + 1$. Obviamente, S não é divisível por nenhum dos p_j, além disso, S é maior do que qualquer p_j. No entanto, pelo Teorema Fundamental da Aritmética ou S é primo ou é composto (possui fator primo em sua decomposição), o que implica na existência de um primo distinto da lista anterior, um absurdo. Logo existem infinitos números primos. ❑

Observação 2.3.5 *Muitas vezes é conveniente representarmos um inteiro "a" utilizando um produtório infinito $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$. Esta representação é sempre possível em virtude da infinitude do conjunto de números primos. Note que se p_k não aparece na representação de a então $\alpha_k = 0$, ou seja, p_k^0, que é igual a 1, elemento neutro da multiplicação.*

Corolário 2.3.2 *Se $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ e $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$, então o m.d.c. $\{a, b\} = \prod_{i=1}^{\infty} p_i^{\gamma_i}$, onde $\gamma_i = min\{\alpha_i, \beta_i\}$.*

Exemplo 2.3.2 *O m.d.c. $\{25, 35\} = m.d.c.\{5^2, 5 \cdot 7\} = 7^0 \cdot 5 = 1 \cdot 5 = 5$.*

2.4 Mínimo Múltiplo Comum

Definição 2.4.1 *O mínimo múltiplo comum de dois inteiros a e b é o menor inteiro positivo que é divisível por a e b. A notação utilizada para o mínimo múltiplo comum de a e b é $m.m.c.\{a,b\}$.*

Lema 2.4.1 *Se $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ e $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$, então o $m.m.c.\{a,b\} = \prod_{i=1}^{\infty} p_i^{\gamma_i}$, onde $\gamma_i = max\{\alpha_i, \beta_i\}$.*

Exemplo 2.4.1 *O $m.m.c.\{9,15\} = m.m.c.\{3^2, 5\cdot 3\} = 3^2 \cdot 5 = 9 \cdot 5 = 45$.*

Proposição 2.4.1 *Se $a, b \in \mathbb{Z}$, então $m.d.c.\{a,b\} \cdot m.m.c.\{a,b\} = ab$.*

Demonstração. Se representarmos $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ e $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$, então

$$ab = \prod_{i=1}^{\infty} p_i^{\alpha_i} \prod_{i=1}^{\infty} p_i^{\beta_i} = \prod_{i=1}^{\infty} p_i^{min\{\alpha_i,\beta_i\}+max\{\alpha_i,\beta_i\}} = \prod_{i=1}^{\infty} p_i^{min\{\alpha_i,\beta_i\}} \prod_{i=1}^{\infty} p_i^{max\{\alpha_i,\beta_i\}} =$$

$$m.d.c.\{a,b\} \cdot m.m.c.\{a,b\} \,. \; \square$$

Observação 2.4.1 *Se $m.d.c.\{a,b\} = 1$, então $m.m.c.\{a,b\} = ab$.*

2.5 Ideais em $\mathbb{Z}$

Agora apresentaremos uma idéia que estará presente em estruturas mais abstratas: ideais em um dado conjunto. No caso estudaremos ideais restritos aos inteiros, sendo de fato uma fonte concreta (simples) de exemplos a fim de auxiliarmos em estudos mais avançados. Veremos que o conceito de ideais em $\mathbb{Z}$ está intimamente ligado ao cálculo de m.d.c.'s. Por fim exibiremos o conceito de ideais maximais e mostraremos como se dá a ligação deste com números primos.

Definição 2.5.1 *Um conjunto de números inteiros I é um ideal de $\mathbb{Z}$ se*

$i_1)$ $0 \in I$;

$i_2)$ *Se* $a, b \in I$, *então* $a + b \in I$;

$i_3)$ *Se* $a \in I$, *então* $-a \in I$;

$i_4)$ *Se* $a \in I$ *e* $t \in \mathbb{Z}$, *então* $ta \in I$.

Exemplo 2.5.1 *O conjunto* $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ *é um ideal de* $\mathbb{Z}$, *já que se verifica*

$i_1)$ $0 = 2 \cdot 0 \in 2\mathbb{Z}$;

$i_2)$ *Se* $a, b \in 2\mathbb{Z}$, *existem* $n, m \in \mathbb{Z}$ *tal que* $a = 2n$ *e* $b = 2m$, *então* $a + b = 2n + 2m = 2(n + m) \in 2\mathbb{Z}$;

$i_3)$ *Se* $a \in 2\mathbb{Z}$, *existe* $n \in \mathbb{Z}$, $a = 2n$, *então* $-a = -2n = 2(-n) \in 2\mathbb{Z}$;

$i_4)$ *Se* $a \in 2\mathbb{Z}$, *existe* $n \in \mathbb{Z}$, $a = 2n$ *e* $t \in \mathbb{Z}$, *então* $ta = t(2n) = 2(tn) \in 2\mathbb{Z}$.

Proposição 2.5.1 *As condições* $i_1)$, $i_2)$ *e* $i_3)$ *podem ser substituídas por*

$i_5)$ $I \neq \varnothing$;

$i_6)$ *Se* $a, b \in I$, *então* $a - b \in I$

Demonstração. Vamos mostrar que se $I \subseteq \mathbb{Z}$ e $i_5)$, $i_6)$ e $i_4)$ são válidas, então I é um ideal de $\mathbb{Z}$.

De fato, se a condição $i_5)$ é válida, então existe $a \in I$ e por $i_6)$ temos que $0 = a - a \in I$, satisfazendo a condição $i_1)$.

Se $a \in I, -a = 0 - a \in I$, por $i_6)$, deste modo a condição $i_3)$ é satisfeita.

Se $a, b \in I$, e por $i_3)$, $-b \in I$, assim, por $i_6)$, temos que $a + b = a - (-b) \in I$, validando $i_2)$. ❑

Exemplo 2.5.2 *Sejam* $n_1, n_2, \ldots, n_k$ *inteiros, o conjunto* $I = n_1\mathbb{Z} + n_2\mathbb{Z} + \ldots + n_k\mathbb{Z} = \{n_1r_1 + n_2r_2 + \ldots + n_kr_k | r_1, r_2, \ldots, r_k \in \mathbb{Z}\}$ *é um ideal de* $\mathbb{Z}$. *pois*

$i_5)$ *De fato, o conjunto* I *é não vazio, por exemplo* $0 \in I$.

$i_6)$ *Se* $a, b \in I$ *existem* $r_1, r_2, \ldots, r_k, l_1, l_2, \ldots, l_k \in \mathbb{Z}$, *onde* $a = n_1r_1 + n_2r_2 + \ldots + n_kr_k$ *e* $b = n_1l_1 + n_2l_2 + \ldots + n_kl_k$. *Deste modo* $a - b = n_1(r_1 - l_1) + n_2(r_2 - l_2) + \ldots + n_k(r_k - l_k) \in I$.

$i_4)$ *Por fim, tome* $t \in \mathbb{Z}$, *então* $ta = t(n_1r_1 + n_2r_2 + \ldots + n_kr_k) = n_1(tr_1) + n_2(tr_2) + \ldots + n_k(tr_k) \in I$. *Logo,* $I = n_1\mathbb{Z} + n_2\mathbb{Z} + \ldots + n_k\mathbb{Z}$ *é um ideal em* $\mathbb{Z}$.

Observação 2.5.1 *Se* $n_1, n_2, \ldots, n_k$ *inteiros, o ideal* $I = n_1\mathbb{Z}+n_2\mathbb{Z}+\ldots+n_k\mathbb{Z}$ *é conhecido como o ideal finitamente gerado por* $n_1, n_2, n_3, \ldots, n_k$, *e denotado por* $[n_1, n_2, \ldots, n_k]$.

Na sequência demonstraremos a existência do chamado ideal principal. Este teorema é importante pois caracteriza todos os ideais em $\mathbb{Z}$.

Teorema 2.5.1 *Todo o ideal* $I \subset \mathbb{Z}$ *é um ideal principal, ou seja, se* I *é um ideal de* $\mathbb{Z}$ *existe* $n \in \mathbb{Z}$ *tal que* $I = n\mathbb{Z}$.

Demonstração. Se $I = \{0\}$, então I é um ideal gerado por 0, ou seja, $I = [0]$.

Suponhamos que $I \neq \{0\}$, então existe $0 \neq x \in I$, por $i_3, -x \in I$, logo $|x|$, pelo P.B.O. existe $n > 0, n \in I$, o menor elemento positivo de I.

Mostremos que $I = n\mathbb{Z}$ ($n\mathbb{Z} \subset I$ e $I \subset n\mathbb{Z}$).

($n\mathbb{Z} \subset I$) Como $n \in I$, por $i_4)$ é claro que $n\mathbb{Z} \subset I$.

($I \subset n\mathbb{Z}$) Seja $a \in I$, "dividindo a por n", utilizando o algoritmo da divisão, existem $q, r \in \mathbb{Z}$, tais que $a = qn + r, 0 \leq r < n$, daí $\underbrace{a}_{a\in I} - \underbrace{qn}_{qn\in I} = r \in I, 0 \leq r < n$ e $n > 0$.

Pela minimalidade de n, $r = 0$, assim:

$a - qn = 0 \Rightarrow a = qn \in n\mathbb{Z}$, logo, $I \subset n\mathbb{Z}$.

Por conseguinte, $I = n\mathbb{Z}$. ❑

Observação 2.5.2 *Assim, o ideal* $n_1\mathbb{Z} + n_2\mathbb{Z} + \ldots + n_k\mathbb{Z}$ *é um ideal principal, ou seja, existe* $n \in \mathbb{Z}$ *tal que* $n_1\mathbb{Z} + n_2\mathbb{Z} + \ldots + n_k\mathbb{Z} = n\mathbb{Z}$.

Exemplo 2.5.3 *Para* $I = 4\mathbb{Z} + 6\mathbb{Z} = \{4n + 6m | n, m \in \mathbb{Z}\} = \{0, \pm2, \pm4, \pm6, \ldots\} = 2\mathbb{Z}$.

Teorema 2.5.2 *Se* $n_1, n_2, \ldots, n_k, d$ *são números inteiros e* d *é tal que* $d\mathbb{Z} = n_1\mathbb{Z}+n_2\mathbb{Z}+\ldots+n_k\mathbb{Z} = n\mathbb{Z}$, *então* $d = m.d.c.\{n_1, n_2, \ldots, n_k\}$.

Demonstração. Inicialmente mostremos que $d|n_1, n_2, \ldots, n_k$. Assim,

$n_i\mathbb{Z} \subset n_1\mathbb{Z} + n_2\mathbb{Z} + \ldots + n_k = n\mathbb{Z} = d\mathbb{Z}, i = 1, 2, \ldots, k$. Logo, $n_i \in d\mathbb{Z}$, ou seja,

$n_i = dl_i$, onde $l_i \in \mathbb{Z}$, assim, $d|n_i$.

Agora mostremos que d é o $m.d.c.\{n_1, n_2, \ldots, n_k\}$. Suponha que d' seja outro $m.d.c.$ de $n_1, n_2, \ldots, n_k$. Se $d'|n_1, n_2, \ldots, n_k$, existem $l_1, l_2, \ldots, l_k \in \mathbb{Z}$, tais que $n_1 = d'l_1; n_2 = d'l_2; \ldots; n_k = d'l_k$. Como $d \in n_1\mathbb{Z} + n_2\mathbb{Z} + \ldots + n_k = n\mathbb{Z}$, existem

$r_1, r_2, \ldots, r_k \in \mathbb{Z}$, onde

$d = n_1r_1 + n_2r_2 + \ldots + n_kr_k = (d'l_1)\, r_1 + (d'l_2)\, r_2 + \ldots + (d'l_k)\, r_k = d'\,(l_1r_1 + l_2r_2 + \ldots + l_kr_k)$, ou seja, $d'|d$, logo d é o $m.d.c.\{n_1, n_2, \ldots, n_k\}$. ❑

Exemplo 2.5.4 $8\mathbb{Z} + 16\mathbb{Z} + 64\mathbb{Z} + 256\mathbb{Z} = 8\mathbb{Z}$, *já que* $m.d.c.\{8, 16, 64, 256\} = 8$.

Definição 2.5.2 *Um ideal* $0 \neq M \subset \mathbb{Z}$ *é dito ser maximal em* $\mathbb{Z}$ *se para qualquer ideal* $I \subset \mathbb{Z}$, *onde* $M \subset I \subset \mathbb{Z}, M = I$ *ou* $\mathbb{Z} = I$, *em outras palavras,* M *é um ideal maximal em* $\mathbb{Z}$ *se não há outro ideal entre* M *e* $\mathbb{Z}$ *em relação a inclusão de conjuntos.*

Exemplo 2.5.5 *O ideal* $2\mathbb{Z}$ *é maximal em* $\mathbb{Z}$. *Considere* $I \subset \mathbb{Z}$ *um ideal tal que* $2\mathbb{Z} \subset I \subset 2\mathbb{Z}$, *e como em* $\mathbb{Z}$ *todos os ideais são principais, existe* $a \in \mathbb{Z}$, *onde* $a\mathbb{Z} = I$. *Observe que* $2 \in I$, *logo existe* $b \in \mathbb{Z}$ *tal que* $2 = ab$. *Como 2 é primo e divide um produto* $2|a$ *ou* $2|b$, *restando as possibilidades:* $a = \pm 2$ *e* $b = \pm 1$, *que neste caso têm-se* $I = 2\mathbb{Z}$ *ou* $a = \pm 1$ *e* $b = \pm 2$, *resultando em* $I = \mathbb{Z}$.

O teorema a seguir relaciona números primos e ideais principais.

Teorema 2.5.3 *Seja* $p \in \mathbb{N}$, *o ideal* $p\mathbb{Z}$ *é maximal em* $\mathbb{Z}$ *se , e somente se,* p *um número primo.*

Demonstração.

($\Rightarrow$) Primeiramente mostremos que p é um número primo, onde, por hipótese, $p\mathbb{Z}$ é um ideal maximal em $\mathbb{Z}$. Suponha que p é composto, ou seja, existem inteiros a, b, onde $1 < a, b < p$, e $p = ab$. Note que $p \in a\mathbb{Z}$, e assim $p\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$, onde $a\mathbb{Z} \neq \mathbb{Z}$, pois $a > 1$, contradizendo a hipótese, logo p é primo.

($\Leftarrow$) Mostremos que $p\mathbb{Z}$ é um ideal maximal em $\mathbb{Z}$, onde, por hipótese, p é um número primo. Se $J \subset \mathbb{Z}$ é um ideal de $\mathbb{Z}$ tal que $p\mathbb{Z} \subset J \subset \mathbb{Z}, J = n\mathbb{Z}$, como $p \in (J = n\mathbb{Z})$, ou

seja, existe $k \in \mathbb{Z}$, onde $p = nk$, logo $n|p$. Como p é primo $n = 1$ ou $n = p$, isto é, $J = p\mathbb{Z}$ ou $J = \mathbb{Z}$. ❑

O teorema acima se faz um critério de primalidade de números, porém não muito eficaz.

Na demonstração do exemplo a seguir faz-se uso dos conceitos estudados de ideais em $\mathbb{Z}$.

Exemplo 2.5.6 *Sejam $a, b, d \in \mathbb{Z}$, e $n \in \mathbb{N}$, em que $d = m.d.c.\{a, b\} = (a, b)$, mostre que $(a^n, b^n) = ((a, b))^n$.*

Demonstração. Sejam $d = (a, b)$ e $c = (a^n, b^n), c \in \mathbb{Z}$, vamos mostrar que $c = d^n$.

Inicialmente, como $d|a, b$ e $d^n|a^n, b^n$, isto implica que $d^n|c$.

Agora iremos mostrar que $c|d^n$.

Como $d^n|a^n, b^n$, $d^n \in a^n\mathbb{Z} + b^n\mathbb{Z} = c\mathbb{Z}$, isto implica que existe $l \in \mathbb{Z}$, onde $d^n = cl$, ou seja, $c|d^n$. ❑

2.6 Equações Diofantinas Lineares

Nesta seção vamos estudar as equações diofantinas lineares, além de um conceito milenar, uma forma de aplicação de *m.d.c.* em $\mathbb{Z}$. Utilizaremos aqui o conceito de ideais em $\mathbb{Z}$ exposto anteriormente.

Definição 2.6.1 *Uma equação diofantina linear é uma equação da forma*

$$ax + by = c, \text{ onde } a, b, c \in \mathbb{Z}.$$

Exemplo 2.6.1 $3x + 11y = 12, 4x - 6y = 17$ *são exemplos de equações diofantinas.*

Salientamos que buscamos encontrar soluções inteiras para tais equações. A seguir veremos a condição para que isto ocorra.

Proposição 2.6.1 *A equação diofantina $ax + by = c$ possui solução em $\mathbb{Z}$ se, e somente se, $d = m.d.c.\{a, b\}$ divide c.*

Demonstração. Sabendo que $I = d\mathbb{Z}$ (todo ideal é principal, Teorema 2.5.1), onde $d = m.d.c.\{a, b\}$ (Teorema 2.5.2), temos que a equação $ax + by = c$ possui solução $x_0, y_0 \in \mathbb{Z}$ se, e somente se, $c = ax_0 + by_0 \in I$, onde o $I = a\mathbb{Z} + b\mathbb{Z} = \{am + bn | m, n \in \mathbb{Z}\}$.

Assim, se $c \in d\mathbb{Z}$, ou seja, existe $e \in d\mathbb{Z}$, onde $c = de$, de modo que $d|c$. ❑

Note que no último exemplo exposto $m.d.c.\{3, 11\} = 1|13$, sendo assim $3x+11y = 13$ tem solução em $\mathbb{Z}$. No entanto, a equação diofantina $4x - 6y = 17$ não dispõe de solução em $\mathbb{Z}$, já que $m.d.c.\{4, -6\} = 2$, e $2 \nmid 17$.

Observação 2.6.1 *Se $d = m.d.c.\{a, b\}|c$ a equação $ax+by = c$ é equivalente a $a'x+b'y = c'$, onde $a' = \frac{a}{d}, b' = \frac{b}{d}$, e $c' = \frac{c}{d}$ assim $m.d.c.\{a', b'\} = 1$. Isto pode auxiliar na simplicação dos cálculos.*

Proposição 2.6.2 *Se (x_0, y_0) é uma solução inteira de $ax + by = c$, então $x' = x_0 + tb$ e $y' = y_0 - ta, t \in \mathbb{Z}$ é também solução de $ax + by = c$.*

Demonstração. Basta substituirmos x' e y' em $ax+by = c$ para encontrarmos $ax'+by' = c$. ❑

Note que x e y são funções de $\mathbb{Z} \times \mathbb{Z}$ na variável t.

Exemplo 2.6.2 *Encontre todas as soluções inteiras de $6x + 102y = 90$.*

Como $d = m.d.c.\{6, 102\} = 6|90$, então $6x + 102y = 90$ possui solução inteira. Uma solução é $x_0 = -2$ e $y_0 = 1$. Portanto, todas as soluções inteiras de $6x + 102y = 90$ são do tipo $x' = -2 + 102t, y' = 1 - 6t$, para t inteiro.

Exemplo 2.6.3 *Em um certo país a moeda é chamada de MERRECA. Neste país há somente duas notas de MERRECA: a de duas MERRECAS e a de três MERRECAS. Se um cidadão deste do país em questão quer pagar em dinheiro uma conta de M$ 51, 00, de que formas isto pode ser feito?*

Nosso problema resume-se a encontrar soluções em inteiros não-negativos para a equação $2x + 3y = 51$. Note que $d = m.d.c.\{2, 3\} = 1$, esta equação tem solução em $\mathbb{Z}$. Como $x_0 = 0$ e $y_0 = 17$ é uma solução particular de $2x + 3y = 51$, a solução geral desta

é dada por $x' = 3t, y' = 17 - 2t$. *Porém, como soluções negativas não fazem sentido para este problema, as soluções possíveis são dadas para* $t \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

CAPÍTULO 3

Congruência e Aritmética Modular

3.1 Introdução

O estudo de congruência foi introduzido por *Carl Friedrich Gauss* (1777-1885) de forma inovadora em sua magnífica obra denominada *Disquisitiones Arithmeticae*, em 1801.

Tal obra foi tão enriquecedora do ponto de vista da área da Teoria dos Números, que muitos estudiosos atribuem o surgimento da Teoria Moderna dos Números a partir da publicação deste livro.

Com o intuito de facilitar o tratamento algébrico de questões envolvendo aritmética dos restos, dispomos do conhecimento dos conceitos, proposições e teoremas relacionados à Congruências, que propiciam ao aluno o entendimento sobre a evolução da matemática ocorrida naquela época, além de permitir ao estudante da área um instrumento poderoso de resolução de inúmeras questões algébricas relacionadas à realidade, sendo que o desconhecimento de tais ferramentas quase necessariamente resultaria em "contas gigantescas" e "difíceis".

Sendo assim, abordaremos a seguir uma relação de equivalência em $\mathbb{Z}$, a relação de congruência módulo m, para $m \in \mathbb{N}, m > 1$.

3.2 Congruência

Definição 3.2.1 *Dados a, b e m inteiros, com $m > 1$, dizemos que "a" é congruente a "b" módulo m e escrevemos $a \equiv b \ mod \ m$, se $m|a - b$.*

Observação 3.2.1 *Se $m \nmid a - b$, então escrevemos que $a \not\equiv b \ mod \ m$ (Lê-se: "a" é incongruente a "b" módulo m).*

Exemplo 3.2.1 $13 \equiv -3 \ mod \ 8$, *pois* $8|13 - (-3) = 16$, *entretanto,* $25 \not\equiv 10 \ mod \ 11$, *pois* $11 \nmid 25 - 10 = 15$.

Demonstraremos a seguir que a relação de congruência módulo m define uma relação de equivalência em $\mathbb{Z}$.

Proposição 3.2.1 *Seja $m \in \mathbb{Z}$, a relação de congruência módulo m, definida em $\mathbb{Z}$, é uma relação de equivalência em $\mathbb{Z}$.*

Demonstração. Para demonstrarmos que a mesma define uma relação de equivalência devemos mostrar as três condições necessárias, que a relação é reflexiva, simétrica e transitiva. Assim, dados $a, b, c, m \in \mathbb{Z}$, temos

i) $m|0 \Rightarrow m|\,(a - a) \Rightarrow a \equiv a \ mod \ m$ (Reflexividade) ;

ii) $a \equiv b \ mod \ m \Rightarrow m|\,(a - b) \Rightarrow m|\,-(a - b) \Rightarrow m|\,(b - a) \Rightarrow b \equiv a \ mod \ m$ (Simetria);

iii) $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m \Rightarrow m|\,(a - b)$ e $m|\,(b - c) \Rightarrow m|\,[(a - b) + (b - c)] \Rightarrow m|a - c \Rightarrow a \equiv c \ mod \ m$ (Transitividade). ❑

Proposição 3.2.2 *Se $a, b, m \in \mathbb{Z}, m > 1, a \equiv b \ mod \ m$ se, e somente se, os restos na divisão euclidiana de a e b por m são iguais.*

Demonstração.

Sejam r_1 e r_2, os restos de a e b na divisão euclidiana por m, respectivamente, logo $a \equiv r_1 \ mod \ m$ e $b \equiv r_2 \ mod \ m$, $r_1 < m$ e $r_2 < m$ assim, $m|a - r_1$ e $m|b - r_2$. Suponha $r_1 \neq r_2$, por hipótese, $a \equiv b \ mod \ m$, temos que $m|a - b$. Como $m|a - r_1$ e $m| - (b - r_2)$ implica que $m|\,[(a - b) + (r_2 - r_1)]$, ora, $m|a - b$, então $m|r_2 - r_1$, absurdo, pois $r_2 - r_1 < m$ e $r_2 - r_1 \neq 0$, já que $r_1 \neq r_2$. Portanto, $r_1 = r_2$. ❑

Proposição 3.2.3 *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$. Então*

1) Se $a \equiv b \ mod \ m$, então $a + c \equiv (b + c) \ mod \ m$;

2) Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a + c \equiv (b + d) \ mod \ m$;

3) Se $a \equiv b \ mod \ m$, então $a \cdot c \equiv (b \cdot c) \ mod \ m$;

4) Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a \cdot c \equiv (b \cdot d) \ mod \ m$

5) Se $a \equiv b \ mod \ m$ e $c > 0$, então $a^c \equiv b^c \ mod \ m$;

6) Se $a + c \equiv (b + c) \ mod \ m$, então $a \equiv b \ mod \ m$;

7) Se $c \neq 0$, $m.d.c.\{c, m\} = 1$ e $a \cdot c \equiv (b \cdot c) \ mod \ m$, então $a \equiv b \ mod \ m$

8) Se $c \neq 0$ e $a \cdot c \equiv (b \cdot c) \ mod \ m$, então $a \equiv b \ mod \ \left(\frac{m}{d}\right)$, em que $d = m.d.c\,\{c, m\}$.

Demonstração. Procederemos a demonstração dos itens ímpares, sendo assim

1) Como $a \equiv b \ mod \ m, m|\,(a - b) = (a + c - c - b) = [(a + c) - (b + c)]$. Portanto, $a + c \equiv (b + c) \ mod \ m$. ❑

3) Tendo em vista $a \equiv b \ mod \ m, m|\,(a - b)$, ou seja, existe $t \in \mathbb{Z}$ tal que $a - b = tm$, multiplicando por c ambos os lados da igualdade, temos que $ac - bc = ctm$, resultando que $m|\,(a \cdot c - b \cdot c)$, assim $a \cdot c \equiv (b \cdot c) \ mod \ m$. ❑

5) Observando a identidade: $a^c - b^c = (a - b)\,(a^{c-1} + a^{c-2}b + \ldots + ab^{c-2} + b^{c-1})$, e sabendo que como $a \equiv b \ mod \ m, m|\,(a - b)$, temos que $m|a^c - b^c$, portanto, $a^c \equiv b^c \ mod \ m$. ❑

7) Como $a \cdot c \equiv (b \cdot c) \ mod \ m, m|\,(a \cdot c - b \cdot c) = [(a-b)\,c]$, como $m.d.c.\,\{c,m\} = 1, m \nmid c$, assim, $m|\,(a-b)$. Portanto, $a \equiv b \ mod \ m$. ❑

Proposição 3.2.4 *A equação de congruência* $ax \equiv 1 \ mod \ m$ *tem solução em* $\mathbb{Z}$*, se, e somente se,* $m.d.c.\,\{a,m\} = 1$.

Demonstração. Note que $ax \equiv 1 \ mod \ m$, assim $m|ax-1$, portanto, existe $y \in \mathbb{Z}$, onde $ax - 1 = my$, ou seja, $ax - my = 1$. Pela proposição 2.6.1, a equação possui solução se existir $d = m.d.c.\,\{a,m\}\,|1$, logo $m.d.c.\,\{a,m\} = 1$. ❑

Definição 3.2.2 *Se* x' *for solução de* $ax \equiv 1 \ mod \ m$, x' *é chamado de inverso multiplicativo de* a *módulo* m.

Exemplo 3.2.2 $x' = 2$ *é inverso multiplicativo de* 4 *módulo* 7*, pois facilmente percebemos que todos os elementos no conjunto* $\{2, 9, 16, 23, \ldots\} \cup \{-5, -12, -19, -26, \ldots\}$ *são inversos multiplicativos de* 4 *módulo* 7.

Observação 3.2.2 *Atentemos que para* p *um número primo, os números* $1, 2, \ldots, p-1$ *são inversíveis módulo* p.

Enunciaremos a seguir um fato importante para os elementos inversíveis módulo p.

Proposição 3.2.5 *Dado* p *um número primo, os únicos elementos auto-inversíveis de um inteiro positivo módulo* p *são apenas os congruentes a* 1 *e* -1 *módulo* p.

Demonstração. Seja x este inteiro positivo, então $x^2 \equiv 1 mod p$, assim

$$x^2 \equiv 1 \ mod \ p \Rightarrow p|x^2 - 1 = (x+1)\,(x-1) \Rightarrow p|\,(x+1) \ \text{ ou } p|\,(x-1).$$

Portanto, os únicos elementos auto-inversíveis módulo p são apenas os congruentes a 1 e -1 módulo p. ❑

Teorema 3.2.1 (Wilson) Se p é um número primo, então $(p-1)! \equiv -1 \ mod \ p$.

Demonstração. Notemos que $(p-1)! = (p-1)(p-2)\cdots 2\cdot 1$. Como $m.d.c.\{a,p\} = 1$ para $1 \leq a \leq p-1$, e temos que cada a neste intervalo é inversível. Como os únicos auto-inversíveis são $p-1$ $(p-1 \equiv -1 \ mod\ p)$ e 1, logo $b = (p-k), 1 < k < p-1$, tem seu inverso na lista $(p-2)(p-3)\ldots 2$. Assim, $(p-1)! \equiv (p-1)\cdot 1 \ mod\ p$, mas $(p-1) \equiv -1 \ mod\ p$. Portanto, $(p-1)! \equiv -1 \ mod\ p$. ❑

Provaremos na sequência a validade da recíproca do teorema de Wilson.

Teorema 3.2.2 *Se $p \in \mathbb{N}$, em que $(p-1)! \equiv -1 \ mod\ p$, então p é um número primo.*

Demonstração. Suponha por absurdo que p não seja primo, ou seja, existem $r, s \in \mathbb{N}$, com $p = rs$, $1 < r, s < p$ e $(p-1)! \equiv -1 \ mod\ p \Rightarrow p|\,(p-1)!+1$. No entanto, notemos que $(p-1)! = (rs-1)!$, assim $(rs-1)! = (rs-1)(rs-2)\cdots(r)\cdots 2\cdot 1$, logo $r|\,(p-1)!$.

Como $r|p$ e $p|\,(p-1)!+1$, temos que $r|\,(p-1)!+1$. Desta forma, se $r|\,(p-1)!+1$ e $r|\,(p-1)!$, resulta que $r|\,(p-1)!+1-(p-1)! = 1$, ou seja $r = 1$, o qual é absurdo pois supomos $r > 1$.

Portanto, p é primo. ❑

Lema 3.2.1 *O produto de k números consecutivos é divisível por $k!$.*

Demonstração. Considere A o produto de k números consecutivos, deste modo $A = n\cdot(n-1)\cdots(n-k+2)\cdot(n-k+1)$. Multiplicando e dividindo por $(n-k)!$ temos que

$$A = \frac{n\cdot(n-1)\cdots(n-k+2)\cdot(n-k+1)\cdot(n-k)!}{(n-k)!}.$$

Desta forma, $A = \dfrac{n!}{(n-k)!}$. Como $\dfrac{A}{k!} = \binom{n}{k}$, sendo assim divisível por $k!$, o que demonstra a afirmação acima. ❑

Lema 3.2.2 *Se p é um número primo então p divide todo número da forma $\binom{p}{k}$, onde $0 < k < p$.*

Demonstração. Para $1 < k < p$, temos que pelo lema anterior $k!$ divide um produto de k números consecutivos, assim $k!|p\cdot(p-1)\cdot(p-2)\cdots(p-k+1)$, e como $m.d.c\,\{k!,p\} =$

1, logo $k!|\,(p-1)\cdot(p-2)\cdots(p-k+1) = \dfrac{(p-1)!}{(p-k)!} \Rightarrow \dfrac{(p-1)!}{(p-k)!k!} = l \in \mathbb{Z}$, portanto, $\binom{p}{k} = pl$, ou seja, $p|\binom{p}{k}$, demonstrando assim o enunciado. ❑

Teorema 3.2.3 (Pequeno Teorema de Fermat - P.T.F.) Se $a, p \in \mathbb{N}$ e p é um número primo, então $a^p \equiv a \ mod\ p$.

Demonstração. Utilizando indução sobre a, temos

i_1) Se $a = 1$, então $1^p = 1 \equiv 1 \ mod\ p$, sendo válido o caso base;

i_2) Suponha válida a proposição $a^p \equiv a \ mod\ p$, então provemos que

$$(a+1)^p \equiv (a+1) \ \ mod\ p.$$

Assim, temos

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + \binom{p}{1} a + \binom{p}{2} a^2 + \ldots + \binom{p}{p-1} a^{p-1} + a^p$$

Pelo lema anterior, temos que $\binom{p}{k} = pl, l \in \mathbb{Z}$, daí
$(a+1)^p = a^p + pl + 1$, como $a^p \equiv a \ mod\ p$, por hipótese, resulta que

$$a^p + 1 \equiv (a+1) \ \ mod\ p.$$

Portanto, $(a+1)^p \equiv (a+1) \ \ mod\ p$. ❑

O resultado a seguir advém do teorema acima demonstrado, em muitas ocasiões seu uso facilita a resolução de problemas envolvendo congruência.

Corolário 3.2.1 *Se $a, p \in \mathbb{N}$ em que p é um número primo e $p \nmid a$, então $a^{p-1} \equiv 1 \ mod\ p$.*

Demonstração. Como $a^p \equiv a \ mod\ p$ e $m.d.c\,\{a, p\} = 1$, temos que

$$p|a^p - a, \text{ então } a^p - a = pq, \text{ para algum } q \in \mathbb{Z}, \text{ assim}$$

$$a\,(a^{p-1} - 1) = pq, \text{ com } p \nmid a, \text{ logo } a^{p-1} \equiv 1 \ mod\ p. \ ❑$$

O exemplo abaixo demonstra o quanto questões aparentemente complexas podem ser resolvidas com uma certa facilidade utilizando os teoremas expostos, ressaltando assim a importância da assimilação de cada conceito para lhe dar com as inúmeras questões acerca de congruência.

Exemplo 3.2.3 *Mostre que* $641|317^{640} + 640!$.

Demonstração. Como $m.d.c\{317, 641\} = 1$, pelo Corolário do P.T.F., resulta que

$$317^{640} \equiv 1 \ mod \ 641.$$

Por Wilson, se $p = 641$ (primo), temos que

$$(641 - 1)! \equiv -1 \ mod \ 641.$$

Somando ambas as congruências:

$$317^{640} + 640! \equiv 0 \ mod \ 641. \ \ \text{❑}$$

3.3 Aritmética Modular

Considerando a relação de equivalência módulo m denotamos o conjunto quociente

$$\frac{\mathbb{Z}}{\equiv mod \ m} \text{ por } \mathbb{Z}_m.$$

Vamos agora introduzir duas operações no conjunto quociente $\dfrac{\mathbb{Z}}{\equiv mod \ m}$. As operações são adição de elementos e o produto de elementos de $\mathbb{Z}_m$, que são herdadas da soma e produto de números inteiros. De fato, vamos somar e multiplicar classes de equivalência que em $\mathbb{Z}_m$ são conjuntos de cardinalidade infinita!

$$\begin{array}{rccc} + : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} \end{array}$$

$$\begin{aligned} . : \quad \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a}.\overline{b} \end{aligned}$$

Com efeito para as operação descritas acima utilizamos as mesmas notações de soma e produto em $\mathbb{Z}$, o que caracteriza um abuso de linguagem matemática, visto que de fato as operações acima são herdadas das operações usuais de $\mathbb{Z}$, este abuso é bem vindo, por hora. Vamos mostrar como obtemos de fato classes que provém de somas e produtos de elementos em $\mathbb{Z}_m$.

A definição a seguir aborda as classes módulo m, para $m > 1$.

Definição 3.3.1 *O conjunto quociente $\mathbb{Z}_m$ é o conjunto $\left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}$.*

Proposição 3.3.1 *Se $\overline{a}, \overline{b} \in \mathbb{Z}_m$ então $\overline{a} + \overline{b} = \overline{a+b}$.*

Demonstração.

$\overline{a} + \overline{b} = \{a' + b' |\ a' \equiv a\ mod\ m \text{ e } b' \equiv b\ mod\ m\}$

$\overline{a+b} = \{c |\ c \equiv (a+b)\ \ mod\ m\}$

Se $d \in \overline{a} + \overline{b} \Rightarrow d = a' + b'$, para $a', b' \in \mathbb{Z}$, onde $a' \equiv a\ mod\ m$ e $b' \equiv b\ mod\ m$, pela Proposição 3.2.3, item ②, $d = a' + b' \equiv (a+b)\ \ mod\ m \Rightarrow d \in \overline{a+b}$, logo $\overline{a} + \overline{b} \subset \overline{a+b}$.

Se $d \in \overline{a+b} \Rightarrow d \equiv (a+b)\ \ mod\ m$. Assim, $d = d - a + a + b - b = d - (a+b) + a + b$. Notemos que $d - (a+b) + a \equiv a\ \ mod\ m$, pois $m | d - (a+b)$ e $b \equiv b\ \ mod\ m$, assim $d = \underbrace{d - (a+b) + a}_{a'} + \underbrace{b}_{b'}$, como $a' \equiv a\ \ mod\ m$ e $b \equiv b\ \ mod\ m$ temos que $d \in \overline{a} + \overline{b}$. Assim, $\overline{a+b} \subset \overline{a} + \overline{b}$. ❑

Observação 3.3.1 *$\overline{m} = \overline{0}$ em $\mathbb{Z}_m$, e também $\overline{km} = \overline{0}, k, m \in \mathbb{Z}$.*

Observação 3.3.2 *Note que se $n \in \mathbb{N}, n\overline{a} = \overline{na}$, pois*

$$n\overline{a} = \underbrace{\overline{a} + \overline{a} + \ldots + \overline{a}}_{n\ \ vezes} = \overline{a + a + \ldots + a} = \overline{na}.$$

E também notemos que $\overline{a^n} = (\overline{a})^n$, pois

$$\overline{a^n} = \underbrace{\overline{a \cdots a}}_{n\ \ vezes} = \underbrace{\overline{a}\overline{a} \cdots \overline{a}}_{n\ \ vezes} = (\overline{a})^n .$$

Definição 3.3.2 *Se $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, então são válidas as seguintes propriedades*

1)(Associatividade na soma) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

2)(comutatividade na soma) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

3)(existência do elemento neutro aditivo) $\overline{a} + \overline{0} = \overline{a}$;

4)(elemento inverso aditivo) Para todo $\overline{a} \in \mathbb{Z}_m$, $\overline{a} + (\overline{-a}) = \overline{0}$;

5)(distributividade) $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac}$;

6)(Associatividade no produto) $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$;

7)(Comutatividade no produto) $\overline{a}\overline{b} = \overline{b}\overline{c}$;

8)(Existência da unidade) $\overline{a}\overline{1} = \overline{a}$.

Proposição 3.3.2 *Se $\overline{a} \in \mathbb{Z}_m$, então $\overline{a}$ é inversível em $\mathbb{Z}_m$ se, e somente se $m.d.c\{a, m\} = 1$.*

Demonstração.

($\Rightarrow$) Se $\overline{a}$ é inversível em $\mathbb{Z}_m$, existe $\overline{b} \in \mathbb{Z}_m$, onde $\overline{a} \cdot \overline{b} = \overline{1}$, assim $\overline{ab} = \overline{1}$, o que implica em $ab \equiv 1 \ mod \ m$, ou seja, existe $k \in \mathbb{Z}$, tal que $ab - 1 = mk$, logo $ab - mk = 1$. Se $d = m.d.c\{a, m\}$, como $d|a, m$, então $d|ab - mk = 1$, logo $d = 1$.

($\Leftarrow$) Se $m.d.c\{a, m\} = 1$, temos que existem $r, s \in \mathbb{Z}$, onde $ar + ms = 1$, utilizando a relação de equivalência módulo m, $\overline{1} = \overline{ar + ms} = \overline{ar} + \overline{ms} = \overline{ar}$ pois $\overline{m} = \overline{0}$, deste modo $\overline{r} = \overline{a}^{-1}$. ❑

Exemplo 3.3.1 *$\overline{4}$ não é inversível em $\mathbb{Z}_8$, pois $4 = m.d.c\{4, 8\}$, porém $\overline{7}$ é inversível em $\mathbb{Z}_8$, pois $m.d.c\{7, 8\} = 1$. No caso, $\left(\overline{7}\right)^{-1} = \overline{7}$.*

Corolário 3.3.1 *Se p é um número primo, todos os elementos não nulos em $\mathbb{Z}_p$ são inversíveis em $\mathbb{Z}_p$.*

Demonstração. Como p é um número primo, se $a \in \mathbb{Z}$, é tal que $1 \leq a < p$, e o $m.d.c\{a, p\} = 1$, logo $\overline{a} \in \mathbb{Z}_p$ é inversível em $\mathbb{Z}_p$. ❑

Corolário 3.3.2 *Se p é primo $\mathbb{Z}_p$ não possui divisores de zero.*

Demonstração. Se $\overline{a}, \overline{b} \in \mathbb{Z}_p$, onde $\overline{a} \cdot \overline{b} = \overline{0}$. Se $\overline{a} \neq \overline{0}$, existe $(\overline{a})^{-1} \in \mathbb{Z}_p$, logo $(\overline{a})^{-1} \cdot (\overline{a}) \cdot \overline{b} = (\overline{a}) \cdot \overline{0} = \overline{0}$, logo $\overline{1} \cdot \overline{b} = \overline{b} = \overline{0}$. Portanto, $\mathbb{Z}_p$, para p primo, não possui divisores de zero. ❑

O Matemático *Pierre de Fermat*, em um de seus escritos estabeleceu que todo número F_n da forma $F_n = 2^{2^n} + 1$ é primo. Outro grande matemático, *Leonhard Euler*, refutou, tempos depois, mostrando que $641|F_5$. Vamos provar que 641 divide F_5 utilizando aritmética modular.

Exemplo 3.3.2 $641|F_5 = 2^{2^5} + 1 = 2^{32} + 1$.

Solução. Observe que

$$\begin{cases} 641 = 2^7.5 + 1 \\ 641 = 2^4 + 5^4 \end{cases}$$

Em $\mathbb{Z}_{641}, \bar{0} = \overline{641} = \overline{2^7.5 + 1} = \overline{2^7.5} + \bar{1} = \bar{2}^7.\bar{5} + \bar{1} = \bar{0}$. Além disso, temos que $\bar{0} = \bar{2}^4 + \bar{5}^4 \Rightarrow \bar{5}^4 = -(\bar{2}^4)$, logo $\bar{2}^7.\bar{5} = \overline{-1} \Rightarrow (\bar{2}^7.\bar{5})^4 = \left(\overline{-1}\right)^4 = \bar{1} \Rightarrow \bar{2}^{28}.\bar{5}^4 = \bar{1}$, substituindo $\bar{5}^4 = -(\bar{2}^4)$, tem-se que $(\bar{2}^{28})\left(\overline{-2}^4\right) = \bar{1} \Rightarrow (\bar{2}^{28})\left(\bar{2}^4\right) = \overline{-1} \Rightarrow$
$\bar{2}^{32} = \overline{-1} \Rightarrow\Rightarrow \bar{2}^{32} + \bar{1} = \overline{2^{32} + 1} = \bar{0} \Rightarrow 2^{32} + 1 \equiv 0 \ mod\ 641$.

A seguir demonstraremos um teorema muito importante para resolução de questões envolvendo congruência e aritmética modular, cujo nome advém do seu autor, denominado Teorema de Euler. Inicialmente, passaremos a definição da função $\phi(n)$.

Definição 3.3.3 *Dado $n \in \mathbb{N}$, a função $\phi(n)$ denota o número de elementos primos com n na lista $1, 2, 3, \ldots, n-1$.*

Observação 3.3.3 *Se m é primo, então $\phi(m) = m - 1$, assim $a^{\phi(m)} = a^{m-1} \equiv 1 mod m$, pelo Pequeno Teorema de Fermat, se $(a, m) = 1$.*

Teorema 3.3.1 (Euler) Se m é um inteiro positivo e a um inteiro em que $(a, m) = 1$, então $a^{\phi(m)} \equiv 1\ mod\ m$.

Demonstração. Se $(a, m) = 1, \mathbb{Z}_m = \left\{\bar{0}, \bar{a}, \overline{2a}, \ldots, \overline{(m-1)\,a}\right\}$, pois se $\bar{l} \in \mathbb{Z}_m$, temos que $0 \leq l < \overline{(m-1)\,a}$, e existe $\bar{j}$ onde $\overline{ja} = \bar{l}$ em $\mathbb{Z}_m$. Para tanto basta $\bar{j} = (\bar{a})^{-1}\,\bar{l}$, pois

$\overline{ja} = \left((\bar{a})^{-1}\,\bar{l}\right)\bar{a} = (\bar{a})^{-1}\,(\bar{a})\,\bar{l} = \bar{l}$.

$\mathbb{Z}_m = \left\{\bar{0}, \bar{a}, \overline{2a}, \ldots, \overline{(m-1)\,a}\right\}$, logo $\bar{a}\cdot\overline{2a}\cdots\overline{(m-1)\,a} = \bar{1}, \overline{2}, \cdots, \overline{(m-1)}$.

Assim, na lista $\bar{a}, \overline{2a}, \ldots, \overline{(m-1)\,a}$, há $\phi(m)$ elementos primos com m. Sejam $\overline{j1a}, \overline{j2a}, \ldots, \overline{j\phi(m)\,a}$ estes elementos. Desta maneira, temos:

$\left(\overline{j1a}\right)\cdot\left(\overline{j2a}\right)\cdots\left(\overline{j\phi(m)\,a}\right) = \overline{j1}\cdot\overline{j2}\cdots\overline{j\phi(m)} \Leftrightarrow$

$\Leftrightarrow \bar{a}^{\phi(m)}\left(\overline{j1}\cdot\overline{j2}\cdots\overline{j\phi(m)}\right) = \overline{j1}\cdot\overline{j2}\cdots\overline{j\phi(m)} \Leftrightarrow$

$\Leftrightarrow a^{\phi(m)} \equiv 1\ mod\ m$. ❑

3.4 Aplicações

3.4.1 Critérios de Divisibilidade

Uma aplicação relevante é a aplicação de congruência nas demonstrações de critérios de divisibilidade.

Geralmente o assunto "Critérios de divisibilidade" é contemplado no 6º ano do ensino fundamental, sendo abordado de forma meramente decoratório, onde se deve lembrar as regras em que a divisibilidade por um número se adequa, não havendo nenhum apreço ao mínimo rigor técnico matemático que justifique os alunos acreditarem no que está escrito nos livros didáticos e cobrados pelo professor.

Além disso, tal assunto é levado adiante e praticamente não é mais cobrado nos conteúdos programáticos das séries posteriores, e essa ausência de preocupação leva o aluno na maioria das vezes a concluir o ensino médio e adentrar o ensino superior sem ter tido o acesso ao "porquê" da validade dos critérios de divisibilidade e como suas demonstrações podem ser relativamente fáceis.

Diante disso, o ensino de congruência e aritmética modular no ensino médio podem auxiliar os alunos e professores no preenchimento dessa lacuna deixada pela problemática curricular.

Inicialmente, seja o número "n" da forma $a_k a_{k-1} a_{k-2} \ldots a_2 a_1 a_0$ na base decimal, com $k \in \mathbb{N}$ ou seja, $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$,

ou seja, $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$. Sendo assim, considerando o número "n" da forma citada, passemos às demonstrações de alguns critérios básicos de divisibilidade:

Divisibilidade por 2

(Linguagem utilizada nos livros didáticos)

Um número é divisível por 2 *quando ele é par.*

(Linguagem utilizando congruência)

Dado $n \in \mathbb{N}$*, se* $2|n$*, então* $a_0 \equiv 0$ *mod* 2.

Demonstração. Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, fatorando as potências de 10 $(2 \cdot 5)$ do lado direito da igualdade temos que:

$$n = a_k \cdot 2^k \cdot 5^k + a_{k-1} \cdot 2^{k-1} \cdot 5^{k-1} + a_{k-2} \cdot 2^{k-2} \cdot 5^{k-2} + \ldots + a_2 \cdot 2^2 \cdot 5^2 + a_1 \cdot 2 \cdot 5 + a_0.$$

Por hipótese, $2|n$, e todas as parcelas do lado direito da igualdade já são divisíveis por 2, exceto a_0, então temos que a proposição se resume a $2|a_0$, ou seja, $a_0 \equiv 0$ *mod* 2. Sendo $a_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (base decimal), assim, a_0 satisfaz a condição acima se for par, ou seja, $0, 2, 4, 6$ ou 8, ou seja, o algarismo da unidade é par. ❑

Exemplo 3.4.1 *Atente que os números* 2456 *e* 1347658 *são divisíveis por* 2*, já que os algarismos da unidade de ambos os números são pares, sendo eles respectivamente,* 6 *e* 8*. No entanto,* 3257 *e* 91215 *não são divisíveis por* 2*, tendo em vista os algarismos da unidade de ambos serem ímpares (*7 *e* 5*, respectivamente).*

Divisibilidade por 3

(Linguagem utilizada nos livros didáticos)

Um número é divisível por 3 *se a soma dos seus algarismos é divisível por* 3*.*

(Linguagem utilizando congruência)

Dado $n \in \mathbb{N}$*, se* $3|n$*, então* $a_k + a_{k-1} + a_{k-2} + \ldots + a_2 + a_1 + a_0 \equiv 0$ *mod* 3.

Demonstração. Tendo em vista que $10 \equiv 1$ *mod* 3, pela proposição 3.2.3, 5, temos

que $10^t \equiv 1^t \ mod\ 3, t \in \mathbb{N}$, ou seja, $10^t \equiv 1 \ mod\ 3$. Como, por hipótese, $3|n$, temos que $n \equiv 0 \ mod\ 3$, mas $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, assim, temos que $\left(a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0\right) \equiv 0 \ mod\ 3$.

Sendo $10^t \equiv 1 \ mod\ 3$, e substituindo em cada parcela acompanhada do fator 10 na congruência exposta, temos que $(a_k \cdot 1 + a_{k-1} \cdot 1 + a_{k-2} \cdot 1 + \ldots + a_2 \cdot 1 + a_1 \cdot 1 + a_0) \equiv 0 \ mod\ 3$, ou seja, $(a_k + a_{k-1} + a_{k-2} + \ldots + a_2 + a_1 + a_0) \equiv 0 \ mod\ 3$. Assim, um número é divisível por 3 se a soma dos seus algarismos é divisível por 3. ❑

Exemplo 3.4.2 *Note que os números* 2556 *e* 73476 *são divisíveis por* 3*, pois a soma dos algarismos de ambos os números resulta em números divisíveis por* 3*, sendo eles respectivamente,* $2+5+5+6 = 18$ *e* $7+3+4+7+6 = 27$*. Entretanto,* 7523 *e* 74285 *não são divisíveis por* 3*, tendo em vista a soma dos algarismos de cada um deles resultar em números não divisíveis por* 3 *(*$7+5+2+3 = 17$ *e* $7+4+2+8+5 = 26$*, respectivamente).*

Divisibilidade por 5

(Linguagem utilizada nos livros didáticos)

Um número é divisível por 5 *se o seu algarismo das unidades for* 0 *ou* 5*.*

(Linguagem utilizando congruência)

Dado $n \in \mathbb{N}$*, se* $5|n$*, então* $a_0 \equiv 0 \ mod\ 5$*.*

Demonstração. Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, fatorando as potências de 10 $(2 \cdot 5)$ do lado direito da igualdade temos que $n = a_k \cdot 2^k \cdot 5^k + a_{k-1} \cdot 2^{k-1} \cdot 5^{k-1} + a_{k-2} \cdot 2^{k-2} \cdot 5^{k-2} + \ldots + a_2 \cdot 2^2 \cdot 5^2 + a_1 \cdot 2 \cdot 5 + a_0$. Como, por hipótese, $5|n$, e todas as parcelas do lado direito da igualdade já são divisíveis por 5, exceto a_0, então temos que a proposição se resume a $5|a_0$, ou seja, $a_0 \equiv 0 \ mod\ 5$. Sendo $a_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (base decimal), assim, a_0 satisfaz a condição acima se for 0 ou 5. ❑

Exemplo 3.4.3 *Observe que os números* 4570 *e* 89345 *são divisíveis por* 5*, tendo em vista os algarismos da unidade dos números ser* 0 *ou* 5*. Em contrapartida, temos que os*

números 9122 *e* 49288 *não são divisíveis por* 5*, tendo em vista os algarismos das unidades de cada um deles não ser múltiplo de* 5 *(*2 *e* 8*, respectivamente).*

Divisibilidade por 7

Definição 3.4.1 *Um número é divisível por* 7 *se a soma de suas classes pares, subtraída da soma de suas classes ímpares, resultar em um número divisível por* 7*.*

Observação 3.4.1 *Este critério geralmente não vem descrito nos livros didáticos do 6º ano do ensino fundamental, diante de sua complexidade em relação aos apresentados anteriormente.*

(Linguagem utilizando congruência)

Dado $n \in \mathbb{N}$*, se* $7|n$*, então* $(\ldots - a_{11}a_{10}a_9 + a_8a_7a_6 - a_5a_4a_3 + a_2a_1a_0) \equiv 0 \ mod\ 7$*.*

Demonstração. Como $1000 \equiv -1 \ mod\ 7$, assim, $(10)^3 \equiv -1 \ mod\ 7$. Além disso, pela proposição 3.2.3, 5, $(10^3)^t \equiv (-1)^t \ mod\ 7$, $t \in \mathbb{N} \cup \{0\}$, logo, temos duas possibilidades: $10^{3t} \equiv 1 \ mod\ 7$, para t par, e $10^{3t} \equiv -1 \ mod\ 7$, para t ímpar. Sabendo que $7|n$, por hipótese, logo $n \equiv 0 \ mod\ 7$, temos que: $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, separando n em t classes, temos que $n = \ldots - a_{11}a_{10}a_9 \cdot (10^3)^3 + a_8a_7a_6 \cdot (10^3)^2 - a_5a_4a_3 \cdot (10^3)^1 + a_2a_1a_0 \cdot (10^3)^0$.

Como $n \equiv 0 \ mod\ 7$, decorre que

$\left(\ldots - a_{11}a_{10}a_9 \cdot (10^3)^3 + a_8a_7a_6 \cdot (10^3)^2 - a_5a_4a_3 \cdot (10^3)^1 + a_2a_1a_0 \cdot (10^3)^0\right) \equiv 0 \ mod\ 7$,

assim, da análise feita acima da paridade das classes (par: $1 \ mod\ 7$ e ímpar:$-1 \ mod\ 7$), têm-se que $(\ldots + a_{11}a_{10}a_9 \cdot (-1) + a_8a_7a_6 \cdot 1 + a_5a_4a_3 \cdot (-1) + a_2a_1a_0 \cdot 1) \equiv 0 \ mod\ 7$.

Portanto, $(\ldots - a_{11}a_{10}a_9 + a_8a_7a_6 - a_5a_4a_3 + a_2a_1a_0) \equiv 0 \ mod\ 7$. ❑

Exemplo 3.4.4 *Observe que os números* 2961 *e* 28861 *são divisíveis por* 7*, visto que a diferença entre classe par (no primeiro caso,* 961*, e no segundo caso,* 861*) e a classe ímpar (no primeiro caso,* 2*, e no segundo caso,* 28*) resulta em números divisíveis por* 7*, sendo eles respectivamente,* $961 - 2 = 959$ *e* $861 - 28 = 833$*. No entanto, temos que os números* 13456 *e* 42352 *não são divisíveis por* 7*, tendo em vista os algarismos a diferença*

entre classes par e ímpares (no caso de 13456, $456 - 13 = 443$, *e no caso de* 42352, $352 - 42 = 310$*), resultando em números não divisíveis por* 7.

Divisibilidade por 9

(Linguagem utilizada nos livros didáticos)

Um número é divisível por 9 *se a soma de seus algarismo resultar em um número divisível por* 9.

(Linguagem utilizando congruência)

Dado $n \in \mathbb{N}$, *se* $9|n$, *então* $a_k + a_{k-1} + a_{k-2} + \ldots + a_2 + a_1 + a_0 \equiv 0 \ mod\ 9$.

Demonstração. Como $10 \equiv 1 \ mod\ 9$, pela proposição 3.2.3, 5, temos que $10^t \equiv 1^t \ mod\ 9, t \in \mathbb{N}$, ou seja, $10^t \equiv 1 \ mod\ 9$. Como, por hipótese, $9|n$, temos que $n \equiv 0 \ mod\ 9$, entretanto, $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, assim, temos que

$\left(a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0\right) \equiv 0 \ mod\ 9$.

Sendo $10^t \equiv 1 \ mod\ 9$, e substituindo em cada parcela acompanhada do fator 10 na congruência exposta, temos que

$(a_k \cdot 1 + a_{k-1} \cdot 1 + a_{k-2} \cdot 1 + \ldots + a_2 \cdot 1 + a_1 \cdot 1 + a_0) \equiv 0 \ mod\ 9$, ou seja,

$$(a_k + a_{k-1} + a_{k-2} + \ldots + a_2 + a_1 + a_0) \equiv 0 \ mod\ 9.$$

Assim, um número é divisível por 9 se a soma dos seus algarismos é divisível por 9. ❑

Exemplo 3.4.5 *Observe que os números* 6327 *e* 57942 *são divisíveis por* 9, *já que a soma dos algarismos de ambos os números resultam em números divisíveis por* 9, *sendo eles respectivamente,* $6 + 3 + 2 + 7 = 18$ *e* $5 + 7 + 9 + 4 + 2 = 27$. *Em contrapartida, temos que os números* 7111 *e* 56278 *não são divisíveis por* 9, *pois* $7 + 1 + 1 + 1 = 10$ *e* $5 + 6 + 2 + 7 + 8 = 28$, *ambos os resultados não divisíveis por* 9.

Divisibilidade por 11

Definição 3.4.2 *Um número é divisível por* 11 *se a soma dos algarismos de ordens ímpares, subtraída da soma dos algarismos de ordens pares resultar em um número divisível por* 11*.*

Observação 3.4.2 *Este critério geralmente não vem descrito nos livros didáticos do 6º ano do ensino fundamental, diante de sua complexidade em relação aos apresentados anteriormente.*

(Linguagem utilizando congruência)

Dado $n \in \mathbb{N}$*, se* $11|n$*, então*
$\left(a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots - a_3 + a_2 - a_1 + a_0\right) \equiv 0 \ mod\ 11.$

Demonstração. Como $10 \equiv -1 \ mod\ 11$, pela proposição 3.2.3, 5, temos que $(10)^t \equiv (-1)^t \ mod\ 11$, $t \in \mathbb{N}$, logo, temos duas possibilidades: $10^t \equiv 1 \ mod\ 11$, para t par, e $10^t \equiv -1 \ mod\ 11$, para t ímpar.

Sabendo que $11|n$, por hipótese, logo $n \equiv 0 \ mod\ 11$, sendo $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, temos que

$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \ mod\ 11.$

Assim, da análise feita acima da paridade das classes (par: $1 \ mod\ 11$ e ímpar: $-1 \ mod\ 11$), têm-se que

$\left(a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots + a_3 \cdot (-1) + a_2 \cdot 1 + a_1 \cdot (-1) + a_0 \cdot 1\right) \equiv 0 \ mod\ 11.$

Portanto, $\left(a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots - a_3 + a_2 - a_1 + a_0\right) \equiv 0 \ mod 11$. ❑

Exemplo 3.4.6 *Observe que os números* 1331 *e* 62315 *são divisíveis por* 11*, tendo em vista que a diferença entre a soma dos algarismos de ordem ímpar e a soma dos algarismo de ordem par de cada número resulta em números divisíveis por* 11*, pois* $(1+3)-(3+1) = 4-4 = 0|11$ *e* $(6+3+5)-(2+1) = 14-3 = 11$*, respectivamente. Em contrapartida, temos que os números* 2015 *e* 61997 *não são divisíveis por* 11*, visto que* $(0+5)-(2+1) = 5-3 = 2$ *e* $(6+9+7)-(1+9) = 22-10 = 12$*, ambos os resultados não divisíveis por* 11*.*

CAPÍTULO 4

Proposta de Sequência Didática

O processo de ensino da matemática torna-se cada vez mais um desafio aos educadores da área de uma forma geral, tendo em vista a complexidade na formação atual, assim como pelos diversos gargalos existentes no sistema educacional atual do nosso país que corroboram para que a matemática seja vislumbrada como a disciplina para "poucos aprenderem", criando um estereótipo de "exclusão" do conhecimento.

Sendo assim, é de extrema importância a participação dos estudiosos da área da Educação Matemática, juntamente com todo o arcabouço teórico, no movimento para tentar modificar o quadro de repúdio e rotulação à matemática pelos estudantes nos dias atuais através da inserção de novas ferramentas que propiciem ao educador matemático novas formas de abordagem dos conhecimentos intrínsecos à disciplina, transformando os mesmos, e tornando mais acessível aos estudantes, desenvolvendo assim, um processo educativo amplamente integrador dos componentes da relação de aprendizagem.

Diante disso, neste capítulo elaboramos uma Proposta de Sequência Didática sobre Congruências para aplicação na Educação Básica, com o intuito de orientar docentes interessados em novas abordagens do conhecimento matemático referente ao assunto.

A seguir abordaremos alguns conceitos da Didática da Matemática que norteiam este capítulo e que formam a base teórica para o objeto de destaque nesta obra.

4.1 Alguns conceitos da Didática da Matemática

A Didática da Matemática tem atualmente um papel de destaque no contexto educacional, visto que dispõe de novas abordagens e novas teorias que podem suprir lacunas existentes na disposição do processo de ensino e aprendizagem matemática em seu amplo contexto, consequentemente melhorando a transmissão do conhecimento e viabilizando um conhecimento dinâmico e condizente com o que a matemática enfatiza, isto é, com o rigor lógico-matemático necessário e com as suas aplicações práticas.

Além disso, a Didática da Matemática é considerada uma tendência teórica advinda de uma área de pesquisa educacional mais ampla, que é a Educação Matemática.

Conforme Pais (2002a), podemos definir o objeto de estudo da Didática da Matemática como:

> "a elaboração de conceitos e teorias que sejam compatíveis com a especificidade educacional do saber escolar matemático, procurando manter fortes vínculos com a formação de conceitos matemáticos, tanto em nível experimental da prática pedagógica, como no território teórico da pesquisa acadêmica." (Pais; p. 11)

Entre alguns conceitos importantes da Didática da Matemática para uma transformação eficaz do ensino da matemática destacamos: a transposição didática, o contrato didático e a engenharia didática.

Sendo assim, faremos um breve resumo sobre cada conceito a seguir, para um maior aprofundamento sobre os temas indicamos a leitura de [2], [4] e [8].

4.1.1 Transposição Didática

Entre as ferramentas de transformação da prática educativa no processo evolutivo que se encontra a Didática da Matemática temos a *transposição didática*, introduzida por Yves Chevallard[2].

Sendo o professor responsável por conduzir o processo de ensino, faz-se necessário a escolha de métodos e elementos práticos que propiciem a melhor e mais adequada forma da passagem do saber científico matemático (surgido da pesquisa), ao saber a ensinar (escolha epistemológica dos conhecimentos a serem contemplados pelo aluno), e finalmente ao saber ensinado (efetivamente praticado em sala de aula), nesta perspectiva de adequação se encontra a noção de transposição didática.

Conforme Chevallard (1991), a transposição didática, em uma definição formal, pode ser descrita como:

> "Um conteúdo do conhecimento, tendo sido designado como saber a ensinar, sofre então um conjunto de transformações adaptativas que vão torná-lo apto a tomar lugar entre os objetos de ensino. O trabalho que, de um objeto de ensino, é chamado de transposição didática." (p. 39)

A relação entre transposição e saber é intrínseco, tendo em vista a necessidade um do outro para caracterização de existência do processo educativo, conforme Pais em [4], tem-se que:

[2]Yves Chevallard (1946-) é um matemático francês, considerado uma das figuras mais importantes da Didática da Matemática.

> "Quando falamos da existência de transposição, no sentido cognitivo do termo, podemos relacionar também a existência de um saber associado. Assim como quando reconhecemos a presença de um saber, é natural pensar na existência de movimentos de transposição que permitiram a síntese desse saber." (p. 12)

De uma forma geral, a transposição didática propõe expressar de modo significativo a acessibilidade do conhecimento matemático, em sua verdadeira forma, através de um conjunto de escolhas que permitem uma aprendizagem significativa do estudante, abarcando questões da realidade em que o aluno está inserido, contribuindo para melhores resultados no processo educativo.

4.1.2 Contrato Didático

Assim como a existência de cláusulas em um contrato firmado entre as partes celebrantes, temos as regras e convenções no processo educativo que relaciona docente e discente, sendo tais pactuamentos base da relação mais conhecida como *contrato didático*.

Consoante entendimento de Brosseau[3](1986) , "Chama-se contrato didático o conjunto de comportamentos do professor que são esperados pelos alunos e o conjunto de comportamentos do aluno que são esperados pelo professor [...] Esse Contrato é o conjunto de regras que determinam uma pequena parte explicitamente, mas sobretudo implicitamente, do que cada parceiro da relação didática deverá gerir daquilo que, de uma maneira ou de outra ele terá de prestar conta perante o outro."

Nesta ótica, temos que o contrato didático tem uma ligação direta com a estratégia de ensino abordada, equilibrando a prática educativa diante de diversos fatores, como por exemplo, os objetivos do curso, a realidade escolar, condições de avaliação, etc. Desse modo, a prática de um ensino matemático tradicional, baseado na memorização de

[3]Guy Brousseau (1933-) é um educador matemático francês, um dos pioneiros da didática da matemática, desenvolveu a Teoria das Situações Didáticas.

fórmulas e postura mecanizada do aluno, que em geral é o mais presente no contexto escolar, sugere uma diferença de gerenciamento por parte do professor do que àquela prática seguindo as orientações contidas em *sequências didáticas* organizadas pelo professor, baseada principalmente em situações-problemas relacionadas ao contexto do aluno.

Portanto, podemos perceber o contrato didático como uma parceria estabelecida entre as partes do processo de ensino visando a construção e aquisição do conhecimento na relação didática que se pactua.

4.1.3 Engenharia Didática

A *engenharia didática* se constitui como metodologia de pesquisa com o intuito de analisar situção didáticas amparadas pela Didática da Matemática. Tal termo tem sido utilizado em pesquisas desde a década de 80.

Conforme Michèle Artigue (1988) a engenharia didática pode ser caracterizada "como um esquema experimental baseado sobre *realizações didáticas* em sala de aula, isto é, sobre a concepção, realização, a observação e a análise de sequências de ensino".

Enquanto metodologia de pesquisa podemos ter dois níveis de engenharia didática, o da microengenharia e o da macroengenharia, o primeiro tem objeto de estudo específico, já o segundo tem por objeto a composição de pesquisas de microengenharia em sua complexidade.

Diante do exposto, podemos entender a engenharia didática, conforme entendimento de Régine Douady (1993) como sendo "uma sequência de aula(s) concebida(s), organizada(s) e articulada(s) no tempo, de forma coerente, por um professor-engenheiro para realizar um projeto de aprendizagem para uma certa população de alunos. No decurso das trocas entre professor e alunos, o projeto evolui sob as reações dos alunos e em função das escolhas e decisões do professor".

Sendo assim, baseado nos conceitos acima abordados, e com o intuito de propor algo que possa ser significativo para melhorar a acessibilidade dos discentes ao conteúdo

relacionado à Congruências, construímos a Proposta de Sequência Didática exposta a seguir, baseada em oficinas realizadas com alunos do final do Ensino Médio e alunos de Iniciação à Docência. Ressaltamos que esta proposta não tem o intuito de abarcar todo o conteúdo ou ser uma receita pronta, tendo em vista a necessidade de uma avaliação diagnóstica anterior e contínua do docente em relação à turma que será trabalhada, sendo necessária uma visão crítica sobre todo o contexto educacional em que está inserido. Trata-se então de uma proposta orientadora aos docentes que pretendem dispor do conhecimento sobre Congruências.

4.2 Proposta de Sequência Didática

Conteúdo abordado: Congruências.

Nível sugerido para aplicação: 2º ou 3º ano do Ensino Médio, ou ainda em preparatório para olimpíadas de matemática.

Duração estimada: 5 a 6 aulas de 50 minutos.

Nosso objetivo é realizar uma transposição didática, introduzindo o conceito de congruência à alunos do ensino médio. Para cumprir com este objetivo utilizaremos a ideia de sequências didáticas, sem abdicar da formalização matemática, formando definições precisas e proposições.

Nesta Proposta de Sequência Didática vamos abordar problemas de divisibilidade com o objetivo de definir a partir de um número $n \in \mathbb{N}$, $n > 1$, o conjunto dos inteiros módulo n, $\mathbb{Z}_n$. Na verdade veremos que cada elemento deste conjunto é também um conjunto numérico com cardinalidade infinita.

Através de definições, proposições, teoremas, exercícios chaves e aplicações se propõe um estudo progressivo e dinâmico do conteúdo tratado, elucidando ao estudante diversos pontos que podem ajudá-lo a resolver problemas dos mais variados tipos, inclusive questões relacionadas ao cotidiano, numa abordagem interdisciplinar.

Com o intuito de melhorar a compreensão da proposta, assim como facilitar aos docentes que desejem utilizar esta obra na aplicação em sua sala de aula, esta Sequência Didática está dividida em partes, mais precisamente duas, A e B. Sendo que a *Parte A* aborda os conceitos iniciais de divisibilidade, em um estudo progressivo, para a abordagem de congruência e suas propriedades, contendo vários problemas sobre o assunto. Enquanto a *Parte B* expõe a questão da aritmética módulo m, seus conceitos, propriedades e exercícios.

4.2.1 PARTE A

Problema 1 *Um ano bissexto é um ano composto por* 366 *dias, um dia a mais do que anos normais, que são compostos por* 365 *dias. No calendário adotado pelo nosso país, esse dia extra é acrescentado no final do mês de fevereiro, que tem normalmente 28 dias, mas que nesses anos passam a ter* 29 *dias. Ocorrendo a cada 4 (quatro) anos, esse dia extra tem o intuito de manter o calendário anual ajustado com a translação da Terra e com os eventos sazonais relacionados às estações do ano. Sabendo que um ano é bissexto se o número relativo ao ano for divisível por* 4*, por exemplo,* 1984 *é um ano bissexto, pois* 4 *divide* 1984*, já que* $1984 \div 4 = 496$*. Sendo assim, quantos anos bissextos existem entre* 1986 *e* 2061*, inclusive? Descreva-os.*

Solução. Utilizando o processo de divisibilidade por 4 em todos os anos entre 1986 e 2061, inclusive, temos que o primeiro ano bissexto no período acima questionado é 1988, pois 4 não divide 1986 nem 1987, mas 4 divide 1988, já que $1988 \div 4 = 497$. Assim, como anos bissextos ocorrem a cada 4 anos, temos que os anos bissextos no período são: $1988, 1992, 1996, 2000, 2004, 2008, 2012, 2016, 2020, 2024, 2028, 2032, 2036, 2040, 2044, 2048, 2052, 2056$ e 2060, num total de 19 anos bissextos.

Observação 4.2.1 *Notemos que os discentes resolverão a questão de certa forma utilizando a noção de congruência módulo* 4*, sendo assim, quando da inserção das definições e propriedades sobre congruência deve ser ressaltado todos os problemas anteriores, que envolvem todo o conceito relacionado à congruência.*

Situação-Problema 1 *Verifique a veracidade as afirmações abaixo:*

i) 7 *dividido por* 6 *deixa resto* 1*.*

ii) 7^2 *dividido por* 6 *deixa resto* 1*.*

iii) 7^3 *dividido por* 6 *deixa resto* 1*.*

Sugestão de indagação aos discentes.

Podemos verificar que as afirmações acima são todas verdadeiras!. Então seria possível afirmar que 7^n dividido por 6 deixa resto 1?. Veremos adiante como o estudo de Congruência no ensino básico poderia auxiliar na solução de problemas como este envolvendo restos de divisão de inteiros, assim como alguns problemas relacionados ao conteúdo proposto.

Definição 4.2.1 *O Algoritmo da divisão euclidiana em $\mathbb{Z}$ Dados inteiros a e b, com $b \neq 0$, existem únicos inteiros q e r, onde $a = bq + r$ e $0 \leq r < |b|$.*

No algoritmo da divisão euclidiana q é chamado de quociente da divisão e r de resto da divisão de a por b.

Exemplo 4.2.1 *Se $a = 17$ e $b = 7$, dividindo 17 por 7, encontramos $q = 2$ e $r = 3$.*

Exemplo 4.2.2 *Se $a = 143$ e $b = 13$, dividindo 143 por 13, encontramos $q = 11$ e $r = 0$.*

Exercício 1 *Encontre o quociente e o resto da divisão de*

a) 47 *por* 5

b) 234 *por* 17

Solução. Efetuando a divisão encontramos

a) $q = 9$ e $r = 2$

b) $q = 13$ e $r = 13$

Problema 2 *Alex, Bianca, Ciro e Daniela, sentados em forma de um círculo, decidiram brincar de "perguntas e respostas". Esta brincadeira consiste que a pessoa que vai perguntar deve apontar a abertura de uma garrafa para si e girar a mesma de forma que quando a mesma parar de girar a abertura da garrafa esteja apontando (ou apontando mais próximo) para a pessoa que deve ser dirigida a pergunta (se parar na pessoa que girou a garrafa, ela deve repetir o processo). Conforme a regras da brincadeira, Alex girou*

a garrafa no sentido horário, e logo na sequência a mesma passou por Daniela, Bianca e Ciro. Sabendo que a abertura da garrafa passou por 114 *pessoas depois de deixar de apontar para Alex até parar, então quem deve fazer a pergunta e quem deve responder a mesma.*

Solução. Considerando as pessoas pela letra inicial do nome, temos que depois de deixar de apontar para A a garrafa fez o seguinte percurso: DBCA, repetindo o processo. Como passou por 114 pessoas basta dividir 114 por 4, gerando $q = 28$ e $r = 2$, ou seja, a garrafa deu 28 voltas completas e depois passou por D parando em B. Sendo assim, Alex deve fazer a pergunta e Bianca deve responder a mesma.

Definição 4.2.2 *Se a e b são inteiros e $b \neq 0$, dizemos que a divide b se existir um inteiro c tal que $b = ac$, e escrevemos $a|b$.*

Observação 4.2.2 *Se a não divide b, denotamos esse fato por $a \nmid b$.*

Exemplo 4.2.3 $2|28$ $(28 = 2 \times 14)$, $7|42$ $(42 = 7 \times 6)$, *mas* $3 \nmid 43$.

Exercício 2 *Julgue os itens abaixo em verdadeiro ou falso*

a) $6|182$

b) $11|374$

c) $17 \nmid 1226$

Solução. Somente o item *a*) é falso.

Neste momento, até mesmo pela maturidade matemática que se espera de um estudante das séries finais do ensino médio, é de enorme importância a abordagem da demonstração matemática em sala de aula, em que pese o acompanhamento do professor na construção de toda a demonstração com a sequência lógica da demonstração, o docente deve deixar o espaço para opinião dos alunos e instigar através de comentários pertinentes determinadas situações que propiciem ao estudante o entendimento da demonstração e a força que tem uma demonstração, visto que depois de provada se torna uma verdade irrefutável.

Tente demonstrar os fatos abaixo:

a) $a|a$, para qualquer $a \in \mathbb{Z}$, $a \neq 0$;

b) $a|b$ então $ac|bc$, para $a, b, c \in \mathbb{Z}$, e a, b e c não nulos.

c) Se $ab|ac$ então $b|c$, para $a, b, c \in \mathbb{Z}$, e a, b e c não nulos.

d) Se $a|b$ e $b|c$ então $a|c$.

Demonstração. Passemos a construção das demonstrações:

a) Para todo $a \in \mathbb{Z}$ existe $1 \in \mathbb{Z}$, tal que $a = a \cdot 1$, ou seja, $a|a$.

b) Se $a|b$, por hipótese, $b = ak$, logo $bc = (ak)\, c = akc = k\,(ac)$, ou seja, $ac|bc$

c) Se $ab|ac$, por hipótese, $ac = abk$, como a não nulo, podemos dividir ambos os membros por a, daí $c = bk$, ou seja, $b|c$.

d) Se $a|b$ e $b|c$, temos que $b = al$ e $c = bk$, assim, substituindo a segunda na primeira, temos: $c = (al)k = a(lk)$, ou seja, $a|c$. ❑

Exercício 3 *Prove que se $a|b$ então $a|mb$, para quaisquer $m \in \mathbb{Z}$.*

Demonstração. Se $a|b$, por hipótese, logo $\exists c \in \mathbb{Z}$ tal que $b = ac$, assim:

$$mb = m\,(ac) = mac = a\,(mc), \text{ ou seja, } a|mb. \quad ❑$$

A partir do exercício anterior, é verdade que:

Exercício 4 *Se $a|b$ e $a|c$, então $a|lc + mb$, para quaisquer $l, m \in \mathbb{Z}$. (Prove isto).*

Demonstração. Pelo exercício anterior temos que se $a|b$ então $a|mb$, assim, se $a|c$ então $a|lc$, ou seja existem $y, t \in \mathbb{Z}$ tais que $ay = mb$ e $at = lc$, daí

$$lc + mb = at + ay = a\,(t + y), \text{ ou seja, } a|lc + mb. \quad ❑$$

Exercício 5 *Prove que a lista $a, a + 1, a + 2$ tem um e somente um múltiplo de 3 para qualquer inteiro positivo a.*

O inteiro positivo a tem apenas três possibilidades na divisão por 3, são elas: não deixa resto, caso seja múltiplo de 3; deixa resto 1; e por último deixa resto 2.

Suponha sem perda de generalidade que a deixa resto 1, assim, $a + 1$ deixa resto

2 e $a+2$ não deixa resto, ou seja, é múltiplo de 3, assim, existe um único inteiro positivo na lista $a, a+1, a+2$ que é múltiplo de 3. ❑

Como você já deve ter notado, dado um número inteiro positivo $n > 1$, os restos possíveis na divisão por n de um número a são $0, 1, 2, \ldots n-1$. A partir desta idéia dividiremos o conjunto dos números inteiros em n classes: cada classe representa um resto na divisão por n. Faremos isto utilizando o que chamaremos de relação de congruência módulo n.

Definição 4.2.3 *Dado m inteiro $m > 1$, a e b inteiros dizemos que a é congruente a b e escrevemos $a \equiv b \ mod \ m$, se $m|a-b$.*

Observação 4.2.3 *se $m \nmid a-b$, então escrevemos que $a \not\equiv b \ mod \ m$.*

Exemplo 4.2.4 $17 \equiv 3 \ mod \ 7$, $29 \equiv 5 \ mod \ 12$, $-15 \equiv -3 \ mod \ 6$ *e* $10 \equiv 10 \ mod \ 9$. *Pois,* $7|(17-3) = 14, 12|(29-5) = 24, 6|(-15+3) = -12$ *e* $9|(10-10) = 0$.

Sugestão. Remeter o estudante aos Problemas 1 e 2 expostos anteriormente, que apesar de aparentemente não parecer envolver o conceito de congruência, nada mais é do que congruência módulo 4. Sendo, portanto, outro caminho de resolução do problema que deve ser construído em sala juntamente com os estudantes.

A relação de congruência apresenta certas propriedades como

1) $a \equiv a \ mod \ m$, para qualquer $a \in \mathbb{Z}$.

2) Se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$, para quaisquer $a, b \in \mathbb{Z}$;

3) Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$, para quaisquer $a, b, c \in \mathbb{Z}$;

4) Se $a \equiv b \ mod \ m$ e $c > 0$, então $a^c \equiv b^c \ mod \ m$;

Prove estas propriedades.

Demonstração.

1) $m|0 \Rightarrow m|(a-a) \Rightarrow a \equiv a \ mod \ m$ (Reflexividade) ;

2) $a \equiv b \ mod \ m \Rightarrow m|(a-b) \Rightarrow m|-(a-b) \Rightarrow m|(b-a) \Rightarrow b \equiv a \ mod \ m$ (Simetria);

3) $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m \Rightarrow m|(a-b)$ e $m|(b-c) \Rightarrow m|[(a-b)+(b-c)] \Rightarrow m|a-c \Rightarrow a \equiv c \ mod \ m$ (Transitividade).

4) Observando a identidade: $a^c - b^c = (a-b)\left(a^{c-1} + a^{c-2}b + \ldots + ab^{c-2} + b^{c-1}\right)$, e sabendo que como $a \equiv b \ mod \ m, m|\,(a-b)$, temos que $m|a^c - b^c$, portanto, $a^c \equiv b^c \ mod \ m$. ❑

Sugestão. Remeter esta última propriedade à Situação-Problema 1 desta Parte A, solucionando o problema em conjunto com os discentes.

Exercício 6 *Julgue os itens abaixo em verdadeiro ou falso.*

a) $25 \not\equiv 2 \ mod \ 12$

b) $314 \equiv 34 \ mod \ 51$

c) $2131 \not\equiv 3 \ mod \ 121$

Solução. Somente o item b) é falso.

Exercício 7 *Mostre que* $20^6 \equiv 9 \ mod \ 11$.

Demonstração. Note que $20^2 \equiv 4 \ mod \ 11$, pois $400 \equiv 4 \ mod \ 11$, elevando ao cubo, temos que $\left(20^2\right)^3 \equiv 4^3 \ mod \ 11$, assim, $20^6 \equiv 64 \ mod \ 11$, como $64 \equiv 9 \ mod \ 11$, resulta que $20^6 \equiv 9 \ mod \ 11$. ❑

Exercício 8 *Encontre a tal que* $18 \equiv a \ mod \ 3$.

Solução. Utilizando a definição de congruência, temos que $3|18-a$, ou seja, existe $k \in \mathbb{Z}$, tal que $18 - a = 3k$, assim, $a = 18 - 3k = 3\,(6-k)$, portanto, existe $m \in \mathbb{Z}$, tal que $a = 3m$.

Sugestões de indagações aos discentes.

Existe apenas um único $a \in \mathbb{Z}$ que satisfaz a $18 \equiv a \ mod \ 3$? A sua resposta é válida para todo $b \in \mathbb{Z}$ e $n \in \mathbb{N}$, tal que $b \equiv a \ mod \ n$?

4.2.2 PARTE B

Conforme questionamento surgido no último exercício da Parte A, suscite a seguinte pergunta aos seus alunos, alterando apenas um pouco a anterior.

Exercício 9 *Encontre b tal que $b \equiv 14 mod 5$.*

Solução. Por definição, $5|b-14$, ou seja, existe $k \in \mathbb{Z}$, tal que $b-14 = 5k$, assim $b = 5k+14, k \in \mathbb{Z}$.

Você aqui já deve ter notado que há infinitos valores de a que satisfazem a e b referentes às duas perguntas anteriores.

Note que dados $n \in \mathbb{N}$, e $a \in \mathbb{Z}$, o conjunto dos $b's$ que satisfazem a equação de congruência $b \equiv a \ mod \ n$ são todos os inteiros que deixam resto igual a a na divisão por n.

Deste modo podemos definir:

Definição 4.2.4 *O conjunto de todos os números inteiros que são congruentes a a módulo n, denotado por $\bar{a}$, é chamado de classe de equivalência de $\bar{a}$, módulo n. Simbolicamente*

$$\bar{a} = \{b \in \mathbb{Z} | b \equiv a \ mod \ n\}.$$

Exemplo 4.2.5 *Para encontrar as classes $\bar{0}$ e $\bar{1}$ módulo 4, temos que*

- $\bar{0} = \{a : a \equiv 0 \ mod \ 4\} = \{a : 4|\,(a-0)\} = \{a : a = 4n, n \in \mathbb{Z}\} = \{4n : n \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$.
- $\bar{1} = \{a : a \equiv 1 \ mod \ 4\} = \{a : 4|\,(a-1)\} = \{a : a = 4n+1, n \in \mathbb{Z}\} = \{4n+1 : n \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$.

Exercício 10 *Encontre a classe $\bar{1}$ módulo 2.*

Solução. * $\bar{1} = \{a : a \equiv 1 \ mod \ 2\} = \{a : 2|\,(a-1)\} = \{a : a = 2n+1, n \in \mathbb{Z}\} = \{2n+1 : n \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

Aqui as propriedades que você provou anteriormente:

1) $a \equiv a \ mod \ n$, para qualquer $a \in \mathbb{Z}$.

2) Se $a \equiv b \ mod \ n$, então $b \equiv a \ mod \ n$, para quaisquer $a, b \in \mathbb{Z}$;

3) Se $a \equiv b \ mod \ n$ e $b \equiv c \ mod \ n$, então $a \equiv c \ mod \ n$, para quaisquer $a, b, c \in \mathbb{Z}$;

Tais propriedades serão de muita ajuda para determinar as classes de equivalência.

Nosso objetivo aqui é justificar que dado $n \in \mathbb{N}$, $n > 1$, o conjunto de todas as classes de equivalência módulo n, $\{\bar{a}|a \in \mathbb{Z}\}$ divide o conjunto dos números inteiros em n partes, onde cada parte tem interseção vazia com outra distinta, ou seja duas partes distintas não tem nada em comum. Para falarmos disto vamos introduzir o conceito de partição de um conjunto.

Rigorosamente uma partição P de A é um conjunto de subconjuntos não vazios e disjuntos de A, tais que $\bigcup_{B \in P} B = A$. Dizemos que dois conjuntos C e D são disjuntos se $C \cap D = \emptyset$.

Definição 4.2.5 *Uma partição P de A é um conjunto tal que:*

P_1) Dois conjuntos distintos em P não tem elementos em comum;

P_2) Cada elemento de A está em algum elemento de P.

Exercício 11 *Encontre todas as partição do conjunto $A = \{a, b, c\}$*

Solução. As partições de A são $\{a\}$, $\{b\}$, $\{c\}$.

Exercício 12 *Encontre $\bar{0}$, e $\bar{1}$ módulo 2.*

Solução. Conforme enunciado, temos

* $\bar{0} = \{a : a \equiv 0 \ mod \ 2\} = \{a : 2|\,(a-0)\} = \{a : a = 2n, n \in \mathbb{Z}\} = \{2n : n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$.

* $\bar{1} = \{a : a \equiv 1 \ mod \ 2\} = \{a : 2|\,(a-1)\} = \{a : a = 2n+1, n \in \mathbb{Z}\} = \{2n+1 : n \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

Exercício 13 *Encontre todas as classes de equivalência módulo* 3.

Solução. As classes de equivalência módulo 3 são $\bar{0}, \bar{1}$ e $\bar{2}$, pois $\bar{3} = \bar{0}$, e assim sucessivamente, daí

$$* \ \bar{0} = \{a : a \equiv 0 \ mod \ 3\} = \{a : 3|\,(a-0)\} = \{a : a = 3n, n \in \mathbb{Z}\} =$$

$$\{3n : n \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}.$$

$$* \ \bar{1} = \{a : a \equiv 1 \ mod \ 3\} = \{a : 3|\,(a-1)\} = \{a : a = 3n+1, n \in \mathbb{Z}\} =$$

$$\{3n+1 : n \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}.$$

$$* \ \bar{2} = \{a : a \equiv 2 \ mod \ 3\} = \{a : 3|\,(a-2)\} = \{a : a = 3n+2, n \in \mathbb{Z}\} =$$

$$\{3n+2 : n \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Sugestão aos discentes. No exercício anterior, você notou que, por exemplo $\bar{1} = \overline{-2}$?

Se definirmos o conjunto de todas as classes de equivalência como a seguir, teremos uma partição do conjunto A via a relação de congruência módulo n.

Definição 4.2.6 *Dado um conjunto A e uma relação de congruência módulo n, o conjunto de todas as classes de congruência módulo n , denotada por $\dfrac{\mathbb{Z}}{\equiv mod \ n}$ é o conjunto*

$$\frac{\mathbb{Z}}{\equiv mod \ n} = \{\bar{a} | a \in \mathbb{Z}\}.$$

Exemplo 4.2.6 $\dfrac{\mathbb{Z}}{\equiv mod \ 2} = \{\bar{a} | a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}\}.$

Exercício 14 *Encontre* $\dfrac{\mathbb{Z}}{\equiv mod \ 5}$

Solução. $\dfrac{\mathbb{Z}}{\equiv mod \ 5} = \{\bar{a} | a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$

Sugestões aos discentes. Como você deve ter notado $\bar{a}$ módulo n é um conjunto infinito.

Problema 3 *O Cometa Halley é um cometa brilhante de período intermediário que retorna às regiões interiores do Sistema Solar a cada período que varia entre* 75 *a* 76 *anos,*

aproximadamente. Foi o primeiro cometa a ser reconhecido como periódico, descoberta feita por Edmond Halley em 1696*. Em sua última passagem na órbita terrestre, o Cometa Halley pôde ser observado a olho nu, em* 09/02/1986*, um domingo. Sabendo que a próxima passagem do Cometa Halley será daqui a* 75 *anos e* 169 *dias a partir de* 09/02/1986*, descubra a data e o dia da semana em que ocorrerá a próxima passagem do Cometa Halley na órbita do nosso planeta.*

Solução. Podemos, para melhor compreensão, dividir o problema em dois questionamentos:

1) Qual a data da nova passagem?

Como a próxima passagem do Cometa Halley será daqui a 75 anos e 169 dias a partir de 09/02/1986, temos que em 09/02/2061 completará 75 anos da última passagem, assim, para sabermos a data do evento, basta adicionarmos 169 dias a data de 09/02/2061. Como 2061 não é um ano bissexto, logo o mês de fevereiro deste ano tem 28 dias, assim, temos 19 dias a ser contados em fevereiro, 31 dias em março, 30 dias em abril, 31 dias em maio, 30 dias em junho, completando até o momento 141 dias a mais que 09/02/2061, faltando 28 dias para completar os 169 dias necessários, portanto, a data da próxima passagem é 28/07/2061.

2) Qual é o dia da semana da nova passagem?

Como temos 7 dias na semana, sendo eles: domingo, segunda-feira, terça-feira, quarta-feira, quinta-feira, sexta-feira e sábado, o problema se resume a um problema de congruência módulo 7. Assim, como domingo foi o dia da semana da última passagem, escolhemos o mesmo como o dia base, assim, sendo x o total de dias percorridos da última passagem até a próxima passagem, temos que

$$\text{Domingo} \longmapsto\ x \equiv 0\ mod\ 7$$

$$\text{Segunda-feira} \longmapsto\ x \equiv 1\ mod\ 7$$

$$\text{Terça-feira} \longmapsto\ x \equiv 2\ mod\ 7$$

$$\text{Quarta-feira} \longmapsto\ x \equiv 3\ mod\ 7$$

$$\text{Quinta-feira} \longmapsto\ x \equiv 4\ mod\ 7$$

$$\text{Sexta-feira} \longmapsto \ x \equiv 5 \ mod \ 7$$

$$\text{Sábado} \longmapsto \ x \equiv 6 \ mod \ 7$$

Sendo assim, como temos 75 anos e 169 dias no intervalo entre as duas passagens, temos que descobrir o número de anos bissextos no período que vai de 1986 à 2061. Conforme resolução do Problema 1, existem 19 anos bissextos, assim:

$$75 \cdot 365 + 169 + 19 = 27563 \text{ dias.}$$

Como 27563 dividido por 7 deixa resto 4, temos que $27563 \equiv 4 \ mod \ 7$, ou seja, a próxima passagem se dará no dia 28/07/2061, quinta-feira.

Uma Sugestão de Problema.

No que diz respeito ao conteúdo relacionado à Números complexos, abordado geralmente no 3º ano do Ensino Médio, temos a noção do número i denotado por $i = \sqrt{-1}$. Assim, temos que

$i = \sqrt{-1}; i^2 = -1; i^3 = -\sqrt{-1} = -i; i^4 = 1; i^5 = i^4 \cdot i = 1 \cdot i = i = \sqrt{-1}; i^6 = i^{3^2} = -1; \ldots$

Diante do exposto, calcule as seguintes potências de i

1) i^{85}

2) i^{1000}

3) i^{163}

Solução. Utilizando os conceitos aprendidos sobre congruência, podemos associar um dado expoente $n, n \in \mathbb{N}$ na seguinte congruência módulo 4

$$\sqrt{-1} \longmapsto \ n \equiv 1 \ mod \ 4$$

$$-1 \ \longmapsto \ n \equiv 2 \ mod \ 4$$

$$-i \ \longmapsto \ n \equiv 3 \ mod \ 4$$

$$1 \ \longmapsto \ n \equiv 0 \ mod \ 4$$

Desse modo, temos

1) i^{85}. Como $n = 85$, temos que $85 \equiv 1 \ mod \ 4$, logo $i^{85} = \sqrt{-1}$.

2) i^{1000}. Como $n = 1000$, temos que $1000 \equiv 0 \ mod \ 4$, então $i^{1000} = 1$.

3) i^{163}. Como $n = 163$, temos que $163 \equiv 3 \ mod \ 4$, portanto, $i^{163} = -i$.

CAPÍTULO 5

Considerações Finais

Diante do contexto em que se encontra o ensino da matemática, sendo um paradigma perante a realidade educativa que clama melhores resultados no processo de aprendizagem matemática, faz-se necessária uma reflexão sobre o processo em si e a utilização de novas abordagens que visem contemplar os anseios de uma prática educacional matemática significantemente produtiva.

Conforme este entendimento, este trabalho propõe a transposição didática do Estudo de Congruências, geralmente visto em cursos de nível superior, para a introdução na educação básica, em turmas de Ensino Médio, trazendo mecanismos que facilitam a resoluções de problemas relacionados à realidade. Apesar disso, saliento que esta obra tem o propósito de orientar professores de matemática, além de outros interessados na temática, não sendo apenas um produto pronto e acabado, até mesmo pelas diferentes realidades no contexto educativo e social vivido nos diversos lugares do nosso país.

Por fim, espero ter contribuído para a inserção de novas práticas matemáticas relacionadas ao Ensino de Congruências, que possibilitem uma melhor maneira de condução da aprendizagem matemática no processo educativo.

Referências Bibliográficas

[1] ALEGRI, Mateus. *Notas de aula de Estruturas Algébricas,* Itabaiana-SE, 2014.

[2] D'AMORE, Bruno. *Elementos de didática da Matemática/,* Bruno D'Amore [tradução Maria Cristina Bonomi]. São Paulo: Editora Livraria da Física, 2007.

[3] DANTE, Luiz Roberto. *Projeto Teláris - Matemática.* 6º ano do Ensino Fundamental. 1ª ed. Sâo Paulo: Editora Ática, 2012.

[4] *Educação Matemática: uma (nova) introdução/ Anna Franchi,..., et al; org. Silvia Dias Alcântara Machado* - 3ª ed. revisada, 2 reimpr. - São Paulo: EDUC, 2012.

[5] HEFEZ, Abramo. *Elementos de Aritmética,* Textos Universitários 2ª ed., Rio de Janeiro: SBM, 2011.

[6] IEZZI, Gelson; DOLCE, Oswaldo; MACHADO, Antonio. *Matemática e Realidade.* 6º ano. 8ª ed. São Paulo: Editora Atual, 2013.

[7] GONÇALVES, Adilson. *Introdução à Álgebra,* Projeto Euclides. Rio de Janeiro: Impa, 1999.

[8] MACHADO, Claúdia Rejane. *Teorias de pesquisa em educação matemática: a influência dos franceses.* Disponível em: http://www.mat.ufrgs.br/∼

vclotilde/disciplinas/pesquisa/CLAUDIA_FRANCESES.DOC.pdf. Acesso em 17.02.2015.

[9] NASCIMENTO, Mauri Cunha do ; FEITOSA, Hércules de Araújo. *Elementos da Teoria de Números.* São Paulo: Cultura Acadêmica, 2009.

[10] OLIVEIRA, Krerley Irraciel Martins. *Iniciação à Matemática: um curso com problemas e soluções / Krerley Irraciel Martins e Adán Jose Corcho Fernández.* Rio de Janeiro: SBM, 2010.

[11] SÁ, Ilydio Pereira de. *Aritmética modular e algumas de suas aplicações.* Disponível em: http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf. Acesso em 12.01.2015.

[12] SAMPAIO, João Carlos. *Introdução à teoria dos números: um curso breve /João Carlos Vieira Sampaio e Paulo Antonio Silvani Caetano.* São Carlos: EDUFSCAR, 2008.

[13] SANTOS, José Plinio de Oliveira. *Introdução à teoria dos números.* 3ª ed., Rio de Janeiro: IMPA, 2010.

[14] STRUIK, Dirk Jan. *A concise history of mathematics.* fourth edition revised, New York: Dover Publications, 1987.

[15] WIKIPÉDIA. *A enciclopédia livre.* Disponível em: http://wikipedia.org. Acesso em 10.02.2015.